SOUTH DAKOTA FUSION CENTER

# Privacy, Civil Rights, and Civil Liberties Protection Policy

## Table of Contents

## A. Intent

The South Dakota Fusion Center (hereafter "SDFC") is committed to the responsible and legal compilation and utilization of criminal investigative and criminal intelligence information and other information important to protecting the safety and security of the people, facilities, and resources of the State of South Dakota and the United States. All compilation, utilization, and dissemination of personal data by SDFC participants and source agencies will conform to requirements of applicable state and federal laws, regulations and rules, and to the greatest extent practicable be consistent with Fair Information Practices. The intent of this policy is to abide by all privacy, civil rights and civil liberties guidance issued as part of the Intelligence Reform and Terrorism Prevention Act of 2004, National Fusion Center Guidelines and the National SAR Initiative. All local, state, tribal and federal agencies providing suspicious activity reports (SAR) with a nexus to South Dakota or participating with the SDFC by virtue of submitting, receiving or disseminating SAR information, criminal intelligence or criminal investigative information via the SDFC are required to adhere to the requirements of the SDFC Privacy, Civil Rights, and Civil Liberties Protection Policy ("SDFC Privacy Policy").

## B. Background

The Department of Homeland Security (DHS) defines fusion centers as state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial (SLTT), federal and private sector partners. A Fusion Center is a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the Center with the goal of maximizing the ability to detect, prevent, apprehend and respond to criminal and terrorist activity utilizing an all crimes/all hazards approach. The SDFC is inclusive of and a component within the South Dakota Department of Public Safety, located in Sioux Falls, South Dakota. The SDFC consists of participating federal agencies, state multi-disciplinary partners, local law enforcement, emergency service, and criminal justice agencies. The number and makeup of participant agencies is subject to change. The SDFC is also open to collaboration with private sector entities. Information utilized by the SDFC includes suspicious activity reports documented by local, state, tribal and federal agencies in a variety of systems to include any future SAR component. Suspicious activity is defined as: "Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." Suspicious Activity Reports (SARs) are defined as "official documentation" of suspicious activity. (See Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting, Version 1.5). SARs are meant to offer a standardized means for feeding information repositories. Any patterns identified during SAR review and analysis may be investigated in coordination with the reporting agency and, if applicable, the SDFC. SARs, although investigatory information, are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

## C. Purpose Statement

The mission of the SDFC is to collect, evaluate, analyze, and disseminate information and intelligence data (records) regarding criminal and terrorist activity in the state while protecting privacy, civil rights, civil liberties, and other protected interests. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the Privacy Act of 1974, as amended, and the Organization for Economic Co-operation and Development's (OECD) Fair Information Principles to ensure that the information privacy and other legal rights of individuals and organizations are protected.

The purpose of this privacy, civil rights, and civil liberties (P/CRCL) protection policy is to promote SDFC and user conduct that complies with applicable federal, state, local and tribal law and assists the center and its users in:

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

## D. Policy Applicability and Legal Compliance

All SDFC personnel, participating agency personnel, personnel providing information technology services to the center, staff members in other public agencies, private contractors providing services to the center, and other authorized users who are not employed by the center or a contractor are required to comply with the SDFC's privacy policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including agencies and centers participating in the Information Sharing Environment [ISE]), and participating criminal justice and public safety agencies, as well as to private contractors, private entities, and the general public. The policy is available to all persons required to comply on the Department of Public Safety's website. Failure to comply may result in exclusion from participation with the SDFC and any other remedies allowed by law.

The SDFC will provide a printed or electronic copy of this policy to all SDFC personnel who provide services and will require both an electronic acknowledgement of receipt of this policy and an electronic agreement to comply with this policy and the provisions it contains.

All SDFC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with the following applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to, the U.S. Constitution and state, local, and federal privacy, civil rights, civil liberties, and legal requirements applicable to the SDFC and/or other participating agencies. .

The SDFC has adopted internal operating policies and/or procedures that are in compliance with applicable laws and regulations protecting privacy, civil rights, and civil liberties including but not limited to, The Constitution of the United States and the South Dakota Constitution Article VI (Bill of Rights), Federal law implementing the U.S. Constitution, other applicable Federal law (See Appendix 2), South Dakota Codified Laws (SDCL) Chapter 1-27 (Public Records and Files), SDCL §1-27-1.5 (Certain records not open to inspection and copying), SDCL §49-31-121 et seq. (Confidential Communication Records), SDCL §58-2-40 (Privacy of Medical Records), and SDCL Chapter 15-15A (Court Records).

## E. Privacy Governance and Oversight

Primary responsibility for the operation of the SDFC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, data quality, analysis, destruction, sharing, dissemination, or disclosure of information; and the enforcement of this policy is assigned to the director of the SDFC or the director's designee in the center.

The SDFC has a privacy team to ensure that privacy, civil rights, and civil liberties are protected within the provisions of this policy and within the center's information collection, retention, and dissemination processes and procedures. The team will at least annually review and update the policy in response to changes in law and implementation experience, including the result of audits and inspections.

The SDFC privacy team is comprised of the SDFC Director and a trained Privacy Officer, appointed by the Director of the center, As needed, the team works closely with the DPS attorney. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, and serves as the liaison for the center and for the ISE as needed. The Privacy Officer can be contacted at sdfusioncenter@state.sd.us.

The Privacy Officer ensures that enforcement procedures and sanctions outlined in this policy are adequate and enforced.

## F. Definitions

For primary terms and definitions, refer to Appendix A, Terms and Definitions.

## G. Information Collection and Retention of Information

The SDFC will seek and/or retain information (including "protected attributes") that:

- Is based on a possible threat to public safety or the enforcement of criminal law; or
- Is based on reasonable suspicion that an identifiable 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; or
- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
- Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); and
- The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
- The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

The SDFC may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads (including suspicious activity report (SAR) information), subject to the policies and procedures specified in this policy and the ISE-SAR Functional Standard (Version 1.5.5).

In accordance with applicable laws, guidance, and regulations, the SDFC will not seek or retain, and information-originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations. However, these attributes may be documented in specific suspect descriptions for identification purposes.

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

- The information is protected information (as defined by the ISE Privacy Guidelines), and, to the extent expressly provided in this policy, includes organizational entities.

- The information is subject to local, state, or federal laws restricting access, use, or disclosure.

The SDFC 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:

- Whether the information consists of tips and leads (including SAR data), criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

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

- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect an individual's right of privacy and his or her civil rights and civil liberties.
- 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.

The labels assigned to existing information under Section G will be reevaluated whenever:

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

SDFC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads (including SAR information). SDFC personnel will:

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and

categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.

- Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method that is used for data that rises to the level of reasonable suspicion (for example, "need to know" and "right to know" access or dissemination for personally identifiable information).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Adhere to and follow the center's physical, administrative, and technical security measures that are in place for the protection and security of tips, leads and SAR information. Tips, leads and SARs will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.

The SDFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect information, as well as information privacy, civil rights, and civil liberties.

The SDFC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information in the ISE. Further, the center will provide notice mechanisms, including but not limited to metadata or data fields 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.

The SDFC requires certain basic descriptive information 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, including:

- The name of the originating center, department, component, and subcomponent.
- The name of the agency system from which the information is disseminated.
- The date the information was collected and, where feasible, the date its accuracy was last verified.
- The title and contact information for the person to whom questions regarding the information should be directed.

The SDFC will clearly indicate legal restrictions on information sharing based on information sensitivity or classification.

The SDFC will keep a record of the source of all information collected and retained by the center.

## H. Acquiring and Receiving Information

Information gathering (acquisition) and access and investigative techniques used by the SDFC and affiliated agencies will comply with and adhere to applicable laws and guidance, including, but not limited to, the following regulations and guidelines:

- 28 CFR Part 23 regarding "criminal intelligence information," as applicable.
- Organization for Economic Co-operation and Development's (OECD) Fair Information Practices (under certain circumstances, there may be exceptions to the Fair Information Practices, based, for example, on authorities provided in the federal Privacy Act; state, local and tribal law; or center policy).
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP) (Ver. 2).
- U.S. and South Dakota Constitutions and applicable law referenced in Section D, paragraph 4, of this policy.
- The center will make every reasonable effort to ensure that it complies with current and future state code and the applicable administrative rules, as well as any other regulations that apply to multi-jurisdictional intelligence and information databases.

The SDFC's SAR process provides for human review and vetting to ensure that information is both gathered in an authorized and lawful manner and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

The SDFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, association, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

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

External agencies that access the SDFC's information or share information with the center are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

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

The SDFC will not directly or indirectly receive, seek, accept or retain information from:

- An individual or nongovernmental entity that may receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
- An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

## I. Information/Data Quality Assurance

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

The SDFC will put in place a process for additional fact development during the vetting process where a SAR includes PII and is based on behaviors that are not inherently criminal. The SDFC will articulate additional facts or circumstances to support the determination that the behavior observed is not innocent but rather reasonably indicative of preoperational planning associated with terrorism.

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

As part of its functional process, the SDFC reviews the data quality of information it originates and makes every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

Originating agencies external to the SDFC are responsible for reviewing the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact

person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

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

Originating agencies providing data to the SDFC remain the owners of the data contributed.

## J. Collation and Analysis

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

Information subject to collation and analysis is information as defined and identified in Section G. Information Collection and Retention of Information.

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

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

The SDFC will make all reasonable efforts that all analytical products be reviewed by the Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

## K. Merging Records

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

Information will be merged only by qualified individuals who have successfully completed a background check and possess the appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

If the matching requirements are not fully met but there is reason to believe the records are about the same individual, the information may be associated by the SDFC if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

## L. Sharing and Disclosure

Credentialed, role-based access criteria will be used by the center, as appropriate, to control:

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

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

Access to or disclosure of records retained by the SDFC will only be provided to persons within the SDFC or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of 5 years by the center.

Agencies external to the SDFC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

Records retained by the SDFC may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

Information gathered or collected and records retained by the SDFC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of 5 years by the center.

Information gathered or collected and records retained by the SDFC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may only be disclosed in accordance with the law and procedures applicable to the SDFC for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center pursuant to center policy and procedure.

Information gathered or collected and records retained by the SDFC will not be:

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

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

- Records required to be kept confidential by law or are exempted from disclosure requirements under SDCL §1-27-1.5.
- Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606 and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
- Investigatory records of law enforcement agencies that are exempted from disclosure requirements under SDCL §1-27-1.5(5).
- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under SDCL §1-271.5(8). This includes a record assembled, prepared or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments under SDCL §1-27-1.5(17).
- Protected federal state, local or tribal records which may include records originated and controlled by another agency that cannot, under SDCL §1-27-1.5(27), be shared without permission.

- A record, or part of a record that constitutes trade secrets or information that is commercial, financial, or otherwise subject to a nondisclosure agreement that was obtained from a person and is privileged and confidential, SDCL 1-27-1.5(3).

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

## M. Redress

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

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

- Disclosure would interfere with, compromise or delay an ongoing investigation or prosecution [SDCL §1-27-1.5(5)];
- Disclosure would endanger the health or safety of an individual, organization or community [SDCL §1-27-1.5(23)];
- The information is in a criminal intelligence information system subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)];
- The information relates to SDCL §1-27-3;
- The information source does not reside with SDFC.
- The SDFC did not originate and/or does not own and does not have a right to disclose the information.

If the information does not originate with the center, the requestor will be referred to the originating agency, if appropriate or required, or the center will notify the source agency of the request and its determination that disclosure by the center or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

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

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

the originating agency. The individual will also be informed of the procedure for appeal when the center or originating agency has cited an exemption for the type of information requested or has declined to disclose information or to correct challenged information to the satisfaction of the individual about whom the information relates.

The ISE Privacy Guidelines require the SDFC to adopt redress procedures when a complaint involves records that have not been disclosed to the complainant under applicable law.

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

(a) Is exempt from disclosure,

(b) Has been or may be shared through the ISE,

(1) Is held by the SDFC and

(2) Allegedly has resulted in demonstrable harm to the complainant,

The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer at the following address: sdfusioncenter@state.sd.us. 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. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

To delineate protected information shared through the ISE from other data, the SDFC maintains records of agencies sharing terrorism-related information and employs system mechanisms whereby the source is identified within the information record.

## O. Security Safeguards

The SDFC Director will designate an appropriately trained individual to serve as the SDFC Security Officer.

SDFC is committed to protecting privacy and maintaining the integrity and security of personal information. SDFC and the South Dakota Bureau of Information and Telecommunications (BIT) shall be responsible for implementing the following security requirements for its intelligence systems:

- Firewalls are in place to prevent unauthorized agencies or entities from accessing SDFC resources.
- SDFC utilizes various levels of Role-Based User Access
    - Each user's role shall determine the types of information accessible to the user. Access to SDFC information will only be granted to center personnel whose positions and job duties require such access and who have successfully completed a background check and appropriate security clearance, if applicable, and who have been selected, approved and trained accordingly
    - Each user's role contains certain permissions to modify or delete records.
- Security Breach Notifications – SDFC and BIT will monitor and respond to security breaches or breach attempts
    - In the event that SDFC personnel become aware of a breach of the security of unencrypted personal information, SDFC will notify any individual whose personal information was or is believed to have been obtained by an unauthorized person and access to which threatens reputational, physical, or financial harm to the person.
    - Any necessary notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.
- Physical Safeguards – SDFC systems shall be located in a physically secured area that is restricted to designated authorized personnel.
    - Only designated, authorized personnel will have access to information stored in the SDFC data systems.
    - All authorized registered visitors will be escorted by designated authorized personnel for the duration of the visit.
- The SDFC Director and BIT Chief Information Security Officer (CISO), or their designees, will identify technical resources to establish a secure facility for center operations with restricted electronic access and alarm systems to guard against external breach of the facility. In addition, the SDFC Director and BIT CISO, or their designees, will identify technological support to develop secure internal and external safeguards against network intrusion of the center's data systems. Access to the center's databases from outside of the facility will only be allowed over secure networks or networks approved by BIT.
- Disaster Recovery – BIT shall maintain appropriate disaster recovery procedures for SDFC data as outlined in their incident response plans.

- The SDFC 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 SDFC will utilize watch logs to maintain audit trails of requested and disseminated information.
- To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data. Risk and vulnerability assessments are not available to the public under SDCL 1-27-1.5(8).

## P. Information Retention and Destruction

All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23. When information is misleading, obsolete or otherwise unreliable, it will be purged, destroyed and deleted or returned to the submitting source. Permission to destroy or return information or records will be presumed if the applicable information is not validated within the specified time. Notification of proposed destruction or return of records may or may not be provided to the contributor by the SDFC, depending on the relevance of the information and any agreement with the providing agency.

Criminal intelligence information and requests for information will be deleted (purged) from the records management system (RMS) periodically if, after holding the information for five (5) years, no updated criminal activity has been documented.

Each entry into the RMS will be evaluated on its own content and may be retained if it is the opinion of the SDFC Director, or his designee, that retention of the information serves a valid law enforcement purpose and the information has been updated to comply with the retention schedule.

## Q. Accountability and Enforcement

The SDFC will be open to the public in regard to information and intelligence collection practices. The SDFC's P/CRCL policy will be provided to the public for review, made available upon request, and posted on the center's website at https://fusion.sd.gov.

The SDFC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Officer can be contacted at sdfusioncenter@state.sd.us.

The SDFC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be retained a minimum of five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

The SDFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law.

The SDFC's personnel or other authorized users shall report errors and confirmed or suspected violations of center policies related to protected information to the center's Privacy Officer.

The SDFC's Governance Board will annually receive a report concerning the review of and any updates to the provisions protecting privacy, civil rights and civil liberties contained within this policy. Changes to this policy may include appropriate responses to changes in applicable law, changes in technology, changes in the purpose and use of the information systems and changes in public expectations.

If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the SDFC Director may:

- Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
- Suspend, demote, transfer, or terminate center personnel, as permitted by applicable personnel policies.
- Apply administrative actions or sanctions as provided by South Dakota Department of Public Safety rules and regulations or as provided in agency/center personnel policies.
- If the authorized user is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

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

## R. Training

The SDFC will require all assigned SDFC personnel and highly encourage participating agency personnel, personnel providing information technology services to the Center, staff members in other public agencies or private contractors providing services to the Center, and authorized users who are not employed by the Center or a contractor to

participate in training programs regarding the implementation of and adherence to the privacy, civil rights and civil liberties policy.

The SDFC will provide special training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

The SDFC's privacy policy training program may include:

- Purposes of this policy;
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing and disclosure of criminal intelligence information and tips and leads information;
- Originating and participating agency responsibilities and obligations under applicable law and policy;
- Implementation of this policy in the day-to-day work of the user, whether a paper or system user;
- Impact of policy violations upon citizens and the agency;
- Mechanisms for reporting violations of center P/CRCL protection policies; and
- Penalties for policy violations;
- How to identify, report, and respond to a suspected or confirmed breach of information held by SDFC;
- Updates to the P/CRCL policy, if any, in response to changes in law and implementation experience; and
- Subject to course availability, the Privacy Officer of the SDFC will also take courses offered by the U.S. Department of Homeland Security addressing privacy, civil rights, and civil liberties training of trainers.

## Appendix I
# Terms and Definitions

**Access—**Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. For data access, access is usually specified as read-only access and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

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

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

**Agency—**See Originating Agency, Owning Agency, Participating Agency, Source Agency, Submitting Agency..

Analysis (law enforcement) — The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment.

**Audit Trail—**Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

**Authentication—**Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process,

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

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

**Biometrics—**A general term used alternatively to describe a characteristic or a process. (1) As a characteristic: a measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition. (2) As a process:

**Center –** Center refers to the SDFC (SDFC), located in Sioux Falls, SD. For operational security reasons, the physical location of the SDFC is not deemed public information.

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

**Civil Rights—** The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federally or state protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.

**Collect—**For purposes of this document, "gather" and "collect" mean the same thing.

**Computer Security—**Protection of information assets through the use of technology, processes, and training.

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

**Credentials—**Information that includes identification and proof of identification that is utilized by SDFC members to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.
Credentialed security access will be utilized to control:

- What information a class of users can have access to;
- What information a class of users can add, change, delete, or print; and
- To whom the information can be disclosed and under what circumstances.

**Criminal Activity—**A behavior, an action, or an omission that is punishable by criminal law.

**Criminal Intelligence Information or Data—**Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

**Data—**Elements of information, inert symbols, signs or measures.

**Data Protection—**Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

**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, compact disk optical media, or cloud technologies.

**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, 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 voice mail.

**Evaluation—**An assessment of the reliability of the source and accuracy of the raw data.

**Fair Information Practice Principles (FIPPS)—**FIPPs are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be limited applicability in intelligence operations, as fusion centers do not generally engage with individuals. That said, fusion centers and all other integrated justice systems should endeavor to apply the FIPPs where practicable.

The eight principles are:
(1) Purpose Specification
(2) Data Quality/Integrity (see definition)
(3) Collection Limitation/Data Minimization
(4) Use Limitation
(5) Security Safeguards (see definition)
(6) Accountability/Audit
(7) Openness/Transparency
(8) Individual Participation

**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.

**Fusion Center—**A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity. The SDFC is the designated state fusion center.

**General Information or Data—**Information that could 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 could be either resolved or unresolved. The record is maintained per statute, rule, or policy.

**Homeland Security Advisor**- Coordinates the efforts in the ongoing assessment of South Dakota's vulnerability to, and ability to detect, prevent, prepare for, respond to, and recover from acts of terrorism within or affecting this state. The South Dakota Homeland Security Advisor is appointed by the Governor and acts in the command position on issues involving homeland security for the state.

**Homeland Security Information—**As defined in Section 892(f)(1) of the Homeland Security Act, homeland security information means any information possessed by a federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual 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 a set of information about a discrete entity that 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 compound of such data as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

**Individual Responsibility—**Since 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—**Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, tips, leads, and SAR data, and criminal intelligence data.

**Information/Data Quality—**Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

**Invasion of Privacy—**Invasion of privacy can be defined as 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.

**Information Sharing Environment (ISE)—** An approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section [1016]. [IRTPA 1016(a)(2)]. The ISE is to provide and facilitate the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. [Extracted from IRTPA 1016(b)(2)]

**ISE-SAR—**A suspicious activity report that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

**ISE-SAR** Information Exchange Package Documentation (IEPD)**—**A schema that facilitates the posting and sharing of ISE-SAR information. The ISE-SAR IEPD is used to represent ISE information in two different data formats:

(1) The Detailed format includes information contained in all data elements set forth in Section IV of the ISE-SAR FS ("ISE-SAR Exchange Data Model"), including fields denoted as privacy fields.

(2) The Summary format excludes certain privacy fields as identified in the ISE-SAR FS. The ISE-SAR FS identifies the minimum privacy fields that must be excluded. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with applicable legal requirements.

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

**Law Enforcement Information—**For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associate with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension,

prosecution, release, detention, adjudication, supervision, or rehabilitation or accused persons or criminal offenders; and victim/witness assistance.

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

**Least Privilege Administration—**A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform.

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

**Maintenance of Information—**The maintenance of information applies to all forms of information storage. This would include 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 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 content. 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 upon the type of information and context of use.

**Need to Know—** As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

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

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

**Owning Agency/Organization—**The organization that owns the target associated with the suspicious activity.

**Participating Agencies—**Participating agencies, for purposes of the EE Initiative, include source [the agency or entity that originates SAR (and, when authorized, ISE-SAR) information], submitting (the agency or entity posting ISESAR information to the shared space), and user (an agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information, including information in the shared space(s), and which may include analytical or operational component(s) of the submitting or authorizing agency or entity) agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

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

**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, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

**Persons—**Executive Order 12333 defines "United States persons" as a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, 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—**Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable 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 Fields—**Data fields in ISE-SAR IEPDs that contain personal information.

**Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy—**A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable 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 agency will adhere to those legal requirements and agency 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 agency, the individual, and the public; and promotes public trust.

**Privacy Protection—**This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing. The process should maximize 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—**For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States.

For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, policy, or other similar instrument should be covered.

For state, local, tribal, and territorial governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable state and tribal constitutions; and applicable state, local, tribal, and territorial laws, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion center or other state, local, tribal, or territorial agency policy or regulation.

**Public—**Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the agency's information;
- Media organizations; and
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency;
- People or entities, private or governmental, who assist the agency in the operation of the justice information system, and agency in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the agency is specified in law.

**Public Access—**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.

**Purge—**A term that is commonly used to describe methods that render data unrecoverable in a storage space or to destroy data in a manner that it cannot be reconstituted. There are many different strategies and techniques for data purging, which is often contrasted with data deletion (e.g., made inaccessible except to system administrators or other privileged users.)

**Reasonably Indicative—**This is operational concept for documenting and sharing suspicious activity takes into account the circumstance in which that observation is made which creates in the mind of the reasonable observer, including law enforcement officer, an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.

**Record—**Any item, collection, or grouping of information that includes personally identifiable information and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

**Redress—**Internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

**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.

**Retention—**Refer to "Storage."

**Right to Know—**Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, counterterrorism activity, or other lawful and authorized government activity.

**Right to Privacy—**The possible right to be left alone, in the absence of some reasonable public interest in 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 that right.

**Role-Based Authorization/Access—**A type of 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—**Security refers to the range of administrative, technical, and physical 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.

**Sharing—**The act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

**SLT—**State, Local and Tribal

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

**Storage—**In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

(1) Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other computer storage. This meaning is probably more common in the IT industry than meaning

(2) In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

**Source Agency/Organization—**The agency or entity that originates SAR (and, when authorized, ISE-SAR) information. The source organization will not change throughout the life of the SAR.

**Submitting Agency/Organization—**the organization that actuates the push of the ISE-SAR to the NSI community. The submitting organization and the source organization may be the same.

**Suspicious Activity—**Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

**Suspicious Activity Reports (SARs) —** Reports that record the documentation of a suspicious activity. Suspicious activity reports (SARs) are meant to offer a standardized means for feeding information repositories or data mining tools. Any patterns identified during SAR data mining and analysis may be investigated in coordination with the reporting agency and, if applicable, the state designated fusion center. Suspicious activity reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

**Terrorism Information—**Consistent with Section 1016(a)(4) of IRTPA, all information relating to the (A) 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, (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations, (C) communications of or by such groups or

individuals, of (D) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

**Terrorism Related Information—**In accordance with IRTPA, as recently as amended by the 9/11 Commission Act enacted on 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 includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not, technically be cited or referenced as a fourth category of information in the ISE.

**Third Agency Rule—**A traditionally implied understanding among criminal justice agencies that confidential criminal intelligence information, which is exempt from public review, will not be disseminated without the permission of the originator.

**Tips and Leads Information or Data—**Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data.

A tip or lead can result from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information hangs between being of no use to law enforcement and being extremely valuable if time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system similar to data that rises to the level of reasonable suspicion.

**User Agency—**The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information in the shared space(s), which may include analytical or operational component(s) of the submitting or authorizing agency or entity.

**Vet/Vetting –** A two-part process by which a trained law enforcement officer or analyst, to include SDFC personnel, determine the usefulness of a SAR. This process entails checking the facts reported in the SAR as well as ensuring that the SAR meets the set of requirements defined in the current version of the SAR Functional Standard. The first step in the vetting process is for a trained officer or analyst at a Fusion Center to determine whether suspicious activity falls within the criteria set forth in Part B – ISE-SAR Criteria Guidance of the current version of the SAR Functional Standard. These criteria describe behaviors and incidents identified by law enforcement officials and counterterrorism experts from across the country as being indicative of criminal activity associated with terrorism. The second step in the vetting process is for a trained expert to determine, based on a combination of knowledge, experience, available information, and personal judgment whether the information has a potential nexus to terrorism.

## Appendix II
# Federal Law Relevant to Seeking, Retaining, and Disseminating Justice Information

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

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

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

**Confidentiality of Alcohol and Drug Abuse Patient Records**; 42 CFR Part 2, Code of Federal Regulations, Title 42: Public Health, Part 2

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

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

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

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

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

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

**Driver's Privacy Protection Act of 1994**: 18 U.S.C. § 2721

**E-Government Act of 2002**; Pub. L. No. 107-347, 208, 116 Stat. 2899 (2002; OMB (0322 OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy

Provisions of the E-Government Act of 2002)

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 Driver's Privacy Protection Act (DPPA)**; 18USC §§ 2721-2725

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

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

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

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

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

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

**National Child Protection Act of 1993**, Public Law 103-209 (December 20, 1993), 107 Stat. 2490

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

**National Security Act**; Public Law 235, Section 606, in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010

**NIST Special Publication 800-53 (Appendix J) Security and Privacy Controls for Federal Information Systems and Organizations**

**Preparing for and Responding to a Breach of Personally Identifiable Information, OMB Memorandum M-17-12 (January 2017)**

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

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

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

**Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)**

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

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

**U.S. Constitution**, First, Fourth, Fifth, Sixth, and Fourteenth Amendments

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

**Applicants and Recipients of Immigration Relief Under the Violence Against Women Act of 1994 (VAWA),** Public Law 103-322, September 13, 1994, and the Victims of Trafficking and Violence Prevention Act of 2000 (T and U nonimmigrant status for victims of trafficking and other serious crimes), Public Law 106-386, Oct. 28, 2000, 8 U.S.C. § 1367, Penalties for Disclosure of Information