

SOUTH DAKOTA FUSION CENTER

SDFC Privacy Policy

Version 4.0

04 January 2011



This policy details the privacy procedures of the South Dakota Fusion Center (SDFC), participants and source agencies submitting, receiving, or disseminating criminal intelligence or criminal investigative information, including suspicious activity reports (SARs), to the Center and users of the Statewide Intelligence System (LEIN).

Table of Contents

| <u>Topic</u> | <u>Pages</u> |
|---|--------------|
| A. Intent | 3 |
| B. Background | 3 |
| C. Purpose | 4 |
| D. Policy Applicability & Legal Compliance | 4 |
| E. Governance and Oversight | 4 |
| F. Definitions | 5 |
| G. Information Collection and Retention of Information | 5 |
| H. Acquiring and Receiving Information | 8 |
| I. Information Quality Assurance | 9 |
| J. Collation and Analysis | 10 |
| K. Merging Records | 11 |
| L. Sharing and Disclosure | 11 |
| M. Redress | 13 |
| N. Complaints & Corrections | 14 |
| O. Security Safeguards | 15 |
| P. Information Retention and Destruction | 16 |
| Q. Accountability and Enforcement | 16 |
| R. Training | 18 |
| Appendix I Terms and Definitions | 20-32 |
| Appendix 2 Federal Law Relevant to Seeking, Retaining, and Disseminating Justice Information | 33-35 |

A. Intent

The South Dakota Fusion Center (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 Policy.

B. Background

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 South Dakota Fusion Center (SDFC) is inclusive of and a component within the South Dakota Department of Public Safety, State Office of Homeland Security, located in Sioux Falls, South Dakota. The SDFC does and will consist 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 also engages in active outreach to 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 of the South Dakota Law Enforcement Information Network (LEIN). 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 state-designated fusion center. 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 regarding criminal or terrorist activity in the state while following appropriate privacy and civil liberties safeguards as outlined in the principles of 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.

D. Policy Applicability and Legal Compliance

All SDFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users will comply with the SDFC's privacy policy concerning the information the center collects, receives, maintains, stores, archives, 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 SDFC will provide a printed or electronic copy of this policy to all agency and non-agency personnel who provide services and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

All SDFC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, and other authorized users will comply with the following applicable law protecting privacy, civil rights, and civil liberties

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 §49-31-121-126 (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, information 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 designate in the center.

The SDFC is guided by a center-designated privacy committee that liaises with community privacy advocacy groups to ensure that privacy and civil rights are protected within the provisions of this policy and within the center's information collection, retention, and dissemination processes and procedures. The committee 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 committee is guided by an appointed and trained privacy officer, who 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 ISE. The Privacy Officer can be contacted at dpshomelandsecurity@state.sd.us.

The privacy officer will adhere to enforcement procedures for violations of the privacy policy and will ensure that enforcement procedures are adequate.

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 that:

- Is based on the criminal predicate or threat to public safety; or
- Is based upon 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 also retain protected information that is based on a level of suspicion that is less than reasonable suspicion, such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy and the ISE-SAR Functional Standard (Version 1.5).

The SDFC will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in

a particular non criminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders or sexual orientations.

The SDFC will apply labels to all center-originated information to indicate to the accessing authorized user that:

- The information is “protected information” to include personal data on any individual (see Appendix 1, Definitions) and, to the extent expressly provided in this policy, includes organizational entities.
- The information is subject to state and/or federal laws restricting access, use, or disclosure.

The SDFC personnel will, upon receipt of information, assess the information to determine its nature and purpose. Personnel will assign information to categories to indicate the result of the assessment, such as:

- Whether the information is general data, tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category;
- The nature of the source (for example, anonymous tip, trained interviewer or investigator, public records, private sector);
- The reliability of the source (for example reliable, usually reliable, unreliable, unknown); and
- 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 the date and incident number for that year pursuant to applicable limitations on access and sensitivity of disclosure in order to:

- Protect confidential sources and police undercover techniques and methods;
- Not to interfere with or compromise pending criminal investigations;
- Protect an individual’s right of privacy and civil rights and civil liberties; and
- Provide legally required protection 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 classification of existing information will be reevaluated whenever:

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
- There is a change in the use of the information affecting access or disclosure limitations.

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 and suspicious activity report (SAR) information. SDFC personnel will:

- Prior to allowing access to or dissemination of the information assess it for sensitivity and confidence.

- Subject the information to an evaluation 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 failed.
- 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.
- Retain information for one year in order to investigate a tip, lead, or SAR information to determine its credibility and value, assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, meets reasonable suspicion/risen to criminal intelligence) so that an authorized user knows that status and purpose for retention and will retain the information based upon the retention period associated with the disposition label. SAR information that has been vetted may be retained for up to 5 years from its initial date of entry unless validated for an additional retention period.
- 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 attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate 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 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, following regulations and guidelines:

- The center will follow 28 CFR Part 23 with regard to criminal intelligence information.
- The center will adhere to the 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).
- The center will adhere to criminal intelligence guidelines established under the US Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP).
- The center will comply with the 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 legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

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, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

Information gathering and investigative techniques used by the SDFC will be the least intrusive means necessary in the particular circumstance to gather information it is authorized to seek or retain.

External agencies that access the SDFC information or provide information to 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 information provider who may or may not receive a fee or benefit for providing the information if the center knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information; or
- An individual or information provider that the center knows or has reason to believe used prohibited means to gather the information, except as expressly authorized by law or center policy.

I. Information 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.

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

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.

The labeling of retained information will be reevaluated by the SDFC (or the originator) when new information is gathered that has an impact on the center's confidence (source reliability or content validity) in previously retained information.

The SDFC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the center learns that the information 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).

State, local, and tribal agencies, including agencies participating in the ISE, are responsible for reviewing the quality and accuracy of the data accessed by or shared with the center. Originating agencies providing data remain the owners of the data contributed. The SDFC will advise the appropriate data owner, in writing or documented electronic notification, if its data is found to be inaccurate, incomplete, out of date or unverifiable.

The SDFC will use written or documented 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.

J. Collation and Analysis

Information acquired by the SDFC or accessed from the 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 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.

If the matching requirements are not fully met but there is an identified partial match, 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:

- 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.

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, the Regional Fusion Center Network 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 whom the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the center.

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 the specific purposes upon request by persons authorized by law to have

such access and only for those uses or purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of 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 or when there is a legitimate need. 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 contributing agency that such information is subject to re-disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency; or
- Disseminated to unauthorized persons.

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

- Public records required to be kept confidential by law 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 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 §1-27-1.5(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 owned or controlled by another agency that cannot, under SDCL §1-27-1.5(27), be shared without permission.
- A violation of an authorized non-disclosure agreement under SDCL §1-27-1.5.

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

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. 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 South Dakota Fusion did not originate and/or does not own or 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.

N. Complaints and Corrections

If an individual has complaints or objections to the accuracy or completeness of information retained about him or her within a system under the center's control, the SDFC 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 declined to disclose information or to correct challenged information to the satisfaction of the individual about whom the information relates.

If an individual has complaints or objections to the accuracy or completeness of information about him or her that originates within another agency, the SDFC director will notify the originating agency of the complaint or correction request and coordinate with them to ensure that the individual is provided with complaint submission or correction procedures. When the complaint pertains to the correction of a record that has been disclosed to the complainant, the originating agency must consent to the correction, remove the record, or assert a basis for denial in accordance with any public laws. This must be done in sufficient time to permit compliance with deadlines found within public laws. A record will be kept of all complaints and correction requests.

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: dps homeland security@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, 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 the ISE originating agencies the center has access to and employs system mechanisms whereby the source is identified within the information record.

O. Security Safeguards

The SDFC assistant director is designated and trained to serve as the SDFC security officer.



The SDFC will operate in a secure facility protected from external intrusion. The SDFC will utilize secure internal and external safeguards against network intrusions. Access to SDFC databases from outside the facility will only be allowed over secure networks or networks approved by the Director.

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

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.

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.

Queries made to the SDFC data applications will be logged into the data system identifying the user initiating the query.

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. ACAMS will be utilized by the center and information placed in ACAMS will be PCII protected if information deems protection under that system.

The SDFC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens the physical, reputation or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information, and if necessary, to reasonably restore the integrity of any information system affected by this release.

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 has no further value or meets the criteria for removal according to the SDFC's retention and destruction policy it will be purged, destroyed, and deleted or returned to the submitting (originating) source.



The SDFC will delete information or return it to the source, unless it is validated, every five (5) years, in compliance with 28 CFR Part 23.

Permission to destroy or return information or records will be presumed if the applicable information is not validated within the specified time period in accordance with this policy.

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.

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

Q. Accountability and Enforcement

The SDFC will be open to the public in regard to information and intelligence collection practices. The SDFC's privacy policy will be provided to the public for review, made available upon request, and posted on the South Dakota Department of Public Safety Homeland Security web page at http://dps.sd.gov/homeland_security/links.aspx.

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 dps homeland security@state.sd.us.

Queries made to the SDFC data applications will be logged into the data system identifying the user initiating the query.

The SDFC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be retained for 3 years, as required by center SDFC policy, 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 their systems, in provisions of this policy and applicable law. This will include logging access of these systems and random auditing of these systems, as to not establish a pattern of the audits. These audits will be mandated at least annually, and a record of the audit will be maintained by the director (or designee) of the center.

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

The SDFC will annually conduct an audit and inspection of the information contained in its criminal intelligence and information system(s). The audit will be conducted by a designated, independent panel. The independent panel has the option of conducting a random audit, without announcement, at any time and without prior notice to the SDFC. This audit will be conducted in such a manner so as to protect the confidentiality, sensitivity and privacy of the center's criminal intelligence system(s).

The SDFC's privacy committee, in conjunction with the Privacy Officer,) will annually review and update the provisions protecting privacy, civil rights and civil liberties contained within this policy and make appropriate changes in response 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 Director of the SDFC will:

- 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 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 user who fails to comply with applicable restrictions and limitations of the SDFC privacy policy.

R. Training

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

- All assigned personnel of the center,
- Personnel providing information technology services to the SDFC,
- Staff in other public agencies or private contractors providing services to the SDFC, and
- Users who are not employed by the SDFC or a contractor.

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

The SDFC'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 SDFC;
- Originating and participating agency responsibilities and obligations under applicable law and policy;
- How to implement the policy in the day to day work of the user, whether a paper or system user;
- The impact of improper activities associated with infractions accessible within or through the agency;
- Mechanisms for reporting violations of center privacy-protection policies; and
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability and immunity, if any.

Appendix I

Terms and Definitions

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

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/Center—Agency/Center refers to the SDFC and all participating local, state or federal agencies of the SDFC.

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—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

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” is used to imply that the state (or government) has a role in ensuring 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 upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

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 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, or compact disk optical media.

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

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's

(OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These were developed around commercial transactions and the trans-border exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system. They are designed to:

1. Define agency purposes for information to help ensure agency uses of information are appropriate. (“Purpose Specification Principle”)
2. Limit the collection of personal information to that required for the purposes intended. (“Collection Limitation Principle”)
3. Ensure data accuracy. (“Data Quality Principle”)
4. Ensure appropriate limits on agency use of personal information. (“Use Limitation Principle”)
5. Maintain effective security over personal information. (“Security Safeguards Principle”)
6. Promote a general policy of openness about agency practices and policies regarding personal information. (“Openness Principle”)
7. Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency. (“Individual Participation Principle”)
8. Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. (“Accountability Principle”)

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 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 of 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, 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. Non-repudiation 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.

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 ISE-SAR 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 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—Protected information includes Personal Data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the South Dakota constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws and ordinances. Protection may also be extended to organizations by center policy or state, local, or tribal law.

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.

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

Redress—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, or counterterrorism 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 in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
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—The agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

Submitting Agency—The agency or entity providing ISE-SAR information to the shared space.

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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