300.00 DALLAS POLICE DEPARTMENT METRO OPERATIONS SUPPORT AND ANALYTICAL INTELLIGENCE CENTER

Nationwide Suspicious Activity Report (SAR) Initiative (NSI) Privacy, Civil Rights, and Civil Liberties Protection Policy

A. Purpose Statement

The purpose of this Nationwide SAR Initiative (hereafter "NSI") Privacy, Civil Rights, and Civil Liberties Protection Policy (hereafter "Privacy and CR/CL Policy") is to promote **Dallas Police Department Metro Operations Support and Analytical Intelligence Center** (hereafter "M.O.S.A.I.C."), source agency (authorized operational components of the Dallas Police Department, Dallas public safety and other governmental agencies, and private sector entities operating in Dallas), and authorized user agency (hereafter collectively referred to as "participating agencies" or "participants") conduct under the NSI that complies with applicable federal, state, local, and tribal laws, regulations, and policies and assists participants in:

- Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
- Increasing public safety and improving national security.
- Protecting the integrity of systems for the observation and reporting of terrorism-related criminal activity and information.
- Encouraging individuals or community groups to trust and cooperate with the justice system.
- Promoting governmental legitimacy and accountability.
- Making the most effective use of public resources allocated to public safety and other governmental agencies.

B. Policy Applicability and Legal Compliance

1. All participating M.O.S.A.I.C. personnel, including personnel providing information technology services to the M.O.S.A.I.C., private contractors, and other authorized participants will comply with applicable provisions of the M.O.S.A.I.C.'s Privacy and CR/CL Policy concerning personal information, including:
   - SAR information the source agency gathers and submits and M.O.S.A.I.C. collects; and
   - The ISE-SAR information identified, submitted to a shared space, and accessed by or disclosed to M.O.S.A.I.C. personnel or to authorized users.

2. The M.O.S.A.I.C. will make available an electronic copy of its Privacy and CR/CL Policy to all M.O.S.A.I.C. personnel, nonagency personnel who provide services to the M.O.S.A.I.C., and to each source agency and M.O.S.A.I.C. authorized user who will be notified of their required compliance with the provisions of this policy.

3. All M.O.S.A.I.C. personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized participants shall comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. and Texas Constitutions and state, local, and federal privacy, civil rights, and civil liberties legal requirements applicable to the M.O.S.A.I.C. and/or other participating agencies. See Appendix B for a list of applicable legal requirements.

C. Governance and Oversight

1. The M.O.S.A.I.C. Lieutenant will have primary responsibility for: operating the M.O.S.A.I.C.; ISE-SAR information system operations; coordinating personnel involved in the NSI; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing or disclosure of SAR and ISE-SAR information; and enforcing the provisions of this policy.

2. The M.O.S.A.I.C.'s participation in the NSI will be guided by the M.O.S.A.I.C. Lieutenant, or designated representative, who will also be M.O.S.A.I.C.'s trained Privacy Officer responsible for enforcing the provisions of this policy and who, in addition to other responsibilities, will receive reports regarding alleged errors and violations of the provisions of this policy.

D. Terms and Definitions

1. The primary terms and definitions used in this privacy policy are set forth in Appendix A, Terms and Definitions.

E. Information

1. The M.O.S.A.I.C. will seek or retain information which the M.O.S.A.I.C. has determined constitutes "suspicious activity" and which:
   - Is based, on (a) a criminal predicate or (b) a possible threat to public safety, including potential terrorism-related conduct.
   - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents, the resulting justice system response, or the prevention of crime.

- The M.O.S.A.I.C. assures was acquired in accordance with agency policy and in a lawful manner.

2. The M.O.S.A.I.C. agrees not to collect SAR information and the M.O.S.A.I.C. will not retain SAR or ISE-SAR information about any individual that was gathered solely on the basis of that individual's religious, political, or social views or activities; participation in a particular noncriminal organization or lawful event; or gathered on the basis of race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

3. Upon receipt of SAR information, which has been identified, reviewed, verified/vetted and processed through established M.O.S.A.I.C. procedures, designated M.O.S.A.I.C. personnel will:
   - Ensure they have complied with the two-step assessment set forth in the *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR)* (SAR Functional Standard) to determine whether the information qualifies as an ISE-SAR.
   - Enter the information following Information Exchange Package Documentation (IEPD) standards and code conventions to the extent feasible.
   - Provide appropriate labels as required under E.5 and E.6 below.
   - Submit (post) the ISE-SAR to the M.O.S.A.I.C.'s shared space.

Notify the submitter of the SAR (point-of-contact) that it has been identified as an ISE-SAR and submitted to the shared space.

4. The M.O.S.A.I.C. will ensure that certain basic and special descriptive information is entered and electronically associated with ISE-SAR information, including:
   - The name of the submitting Department, agency, or entity.
   - The date the information was submitted.
   - The point-of-contact information for SAR-related data.
   - Information that reflects any special laws, rules, or policies regarding access, use, and disclosure.

5. Information provided in the ISE-SAR shall indicate, to the maximum extent feasible and consistent with the current version of the SAR Functional Standard:
   - The nature of the source: anonymous tip, confidential source, trained interviewer or investigator, written statement (victim, witness, other), private sector, or other source.
   - Confidence levels, including:
     - The reliability of the source:
       - Reliable—the source has been determined to be reliable.

  - Unreliable—the reliability of the source is doubtful or has been determined to be unreliable.
  - Unknown—the reliability of the source cannot be judged or has not as yet been assessed.
- The validity of the content:
  - Confirmed—information has been corroborated by an investigator or other reliable source.
  - Doubtful—the information is of questionable credibility but cannot be discounted.
  - Cannot be judged—the information cannot be confirmed.
- Due diligence will be exercised in determining source reliability and content validity. Information determined to be unfounded will be purged from the shared space.
- Unless otherwise indicated through verification/vetting by the M.O.S.A.I.C., source reliability is deemed to be "unknown" and content validity "cannot be judged." In such case, users must independently confirm source reliability and content validity with M.O.S.A.I.C., the source agency, or validate it through their own investigation.

6. At the time a decision is made to post ISE-SAR information to the shared space, M.O.S.A.I.C. personnel will ensure that the ISE-SAR information is labeled, to the maximum extent feasible and consistent with the SAR Functional Standard, to reflect any limitations on disclosure based on sensitivity of disclosure (dissemination description code), in order to:
   - Protect an individual's right of privacy, civil rights, and civil liberties.
   - Protect confidential sources and police undercover techniques and methods.
   - Not interfere with or compromise pending criminal investigations.
   - Provide any legally required protection based on an 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.

7. The M.O.S.A.I.C. will share ISE-SAR information with authorized non-fusion center agencies and individuals only in accordance with established M.O.S.A.I.C. policy and procedure.

8. The M.O.S.A.I.C. will ensure that ISE-SAR information in the shared space that is not verified (confirmed) will be subject to continuing assessment for confidence by subjecting it to an evaluation or screening process to confirm its credibility and value or categorize the information as unfounded or uncorroborated. If subsequent attempts to validate the information confirm its validity or are unsuccessful, the information in the shared space will

be updated (replaced) to so indicate. Information determined to be unfounded will be purged from the shared space.

9. The M.O.S.A.I.C. will incorporate the gathering, processing, reporting, analyzing, and sharing of SAR and ISE-SAR information (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 the information, as well as the privacy, civil rights, and civil liberties of individuals.

10. Notice will be provided through data field labels or narrative information to enable authorized users to determine the nature of the protected information in the shared space and how to handle the information in accordance with applicable legal requirements, including any restrictions based on information security or classification.

F. Acquiring and Receiving Information

1. Information acquisition and investigative techniques used by source agencies must comply with and adhere to applicable law, regulations, and guidelines, including, where applicable, U.S. and state constitutional provisions, applicable federal and state law provisions, local ordinances, and regulations.

2. Law enforcement officers and other personnel at source agencies who acquire SAR information that may be shared with the M.O.S.A.I.C. will be trained to recognize behavior that is indicative of criminal activity related to terrorism.

3. When a choice of investigative techniques is available, information documented as a SAR or ISE-SAR should be acquired or investigated using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation.

4. Access to and use of ISE-SAR information is governed by the U.S. Constitution, the Texas state constitution, applicable federal and state laws and local ordinances, and Office of the Program Manager for the Information Sharing Environment (PM-ISE) policy guidance applicable to the NSI.

G. Information Quality Assurance

1. The M.O.S.A.I.C. will ensure that source agencies assume primary responsibility for the quality and accuracy of the SAR data collected by the M.O.S.A.I.C.

2. The M.O.S.A.I.C. will make every reasonable effort to ensure that SAR information collected and ISE-SAR information retained and posted to the shared space is dependable and trustworthy and is as accurate, current, and complete as possible.

3. At the time of posting to the shared space, ISE-SAR information will be labeled according to the level of confidence in the information (source reliability and content validity) to the maximum extent feasible.

4. The labeling of ISE-SAR information will be periodically evaluated and updated in the shared space when new information is acquired that has an impact on confidence in the information.

5. Alleged errors or deficiencies (misleading, obsolete, or otherwise unreliable) in ISE-SAR information will be investigated in a timely manner, and any needed corrections to or deletions will be made to such information in the shared space.

6. ISE-SAR information will be removed from the shared space if it is determined the source agency did not have authority to acquire the original SAR information, used prohibited means to acquire it, or if the information is subject to an expungement order in a state or federal court that is enforceable under Texas state law or policy.

7. The M.O.S.A.I.C. will provide written notice (this would include electronic notification) to any user agency that has accessed the ISE-SAR information posted to the shared space when ISE-SAR information posted to the shared space by the M.O.S.A.I.C. is corrected or removed from the shared space by the M.O.S.A.I.C. because it is erroneous or deficient such that the rights of an individual may be affected.

H. Analysis

1. ISE-SAR Information posted by the M.O.S.A.I.C. to the shared space or accessed from the shared spaces under the NSI will be analyzed for intelligence purposes only by qualified M.O.S.A.I.C. personnel who have successfully completed a background check and any applicable security clearance and have been selected, approved, and trained accordingly (including training on the implementation of this policy). These personnel shall share ISE-SAR information only through authorized analytical products.

2. ISE-SAR information is analyzed according to priorities and needs, including analysis to:
   - Further terrorism prevention, investigation, force deployment, or prosecution objectives and priorities established by the M.O.S.A.I.C. or the Dallas Police Department.

- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in terrorism-related activities.

I. Sharing and Disclosure

1. Credentialed, role-based access criteria will be used, as appropriate, to determine which system users will be authorized to view privacy fields in ISE-SAR information in response to queries made through a federated ISE-SAR search.

2. Unless an exception is expressly approved by the PM-ISE, the M.O.S.A.I.C. will adhere to the SAR Functional Standard for the ISE-SAR process, including the use of the ISE-SAR IEPD reporting format, NSI approved data collection codes, and ISE-SAR information sharing and disclosure business rules.

3. ISE-SAR information retained by the M.O.S.A.I.C. and entered into the M.O.S.A.I.C.'s shared space will be accessed by or disseminated only to persons within the M.O.S.A.I.C. or, as expressly approved by the PM-ISE, users who are authorized to have access and need the information for specific purposes authorized by law. Except as provided in J.1. below, access and disclosure of personal information will only be allowed to agencies and individual users for legitimate law enforcement and public protection purposes and only for the performance of official duties in accordance with law.

4. ISE-SAR information posted to the shared space by the M.O.S.A.I.C. may be 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 M.O.S.A.I.C. mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the M.O.S.A.I.C. for this type of information.

5. ISE-SAR information **will not be provided** to the public if, pursuant to applicable law (constitutional. statutory, or judicial decision), including the Public Information Act, Texas Government Code, Chapter 552, it is:
   - Required to be kept confidential or exempt from disclosure.
   - Classified as information or records that are exempt from disclosure.
   - Protected federal, Texas state, or tribal records originated and controlled by the M.O.S.A.I.C. that cannot be shared without permission.
   - A violation of an authorized nondisclosure agreement.

6. The M.O.S.A.I.C. will not confirm the existence or nonexistence of ISE-SAR information to any person, organization, or other entity not otherwise entitled to receive the information.

J. Disclosure and Correction/Redress

J.1. Mandatory Disclosure and Correction

1. The M.O.S.A.I.C. is subject to the Public Information Act, Texas Government Code, Chapter 552, which gives the public access to government records by establishing a presumption that it will be made available. Under the law, information may only be withheld if an exception, established by constitution, statute, or court decision, applies. The government agency, to obtain an exception, must make a written request to the Attorney General for an opinion on the exception requested within 10 business day of receiving the request for disclosure. The Attorney General then has 45 days to make a decision. A requestor may provide a written argument for release. In the event of an adverse determination, a government agency may not request reconsideration of an adverse decision.

2. The primary law enforcement provision of Chapter 552 is at Sec. 552.108 (a) and (b) (See Appendix B).

J.2. Redress (Complaint and correction when no right to disclosure)

1. If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information about him or her that is alleged to be held by the M.O.S.A.I.C., the M.O.S.A.I.C., as appropriate, will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

2. The M.O.S.A.I.C. will acknowledge the complaint and state that it will be reviewed but will not confirm the existence of any ISE-SAR that contains information in privacy fields that identifies the individual. However, any personal information will be reviewed and corrected in or deleted from the ISE-SAR shared space if the information is determined to be erroneous, includes incorrectly merged information, or is out of date.

K. Security Safeguards

1. The M.O.S.A.I.C.'s Lieutenant is designated and trained to serve as the M.O.S.A.I.C.'s security officer for the NSI.

2. The M.O.S.A.I.C. will operate in a secure facility protecting the facility from external intrusion. The M.O.S.A.I.C. will utilize secure internal and external safeguards against network intrusions of ISE-SAR information. Access to the M.O.S.A.I.C.'s ISE-SAR shared space from outside the facility will be allowed only over secure networks.

3. The M.O.S.A.I.C. will secure ISE-SAR information in the M.O.S.A.I.C.'s shared space in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by M.O.S.A.I.C. personnel authorized to take such actions.

4. Access to ISE-SAR information will be granted only to M.O.S.A.I.C. personnel: whose positions and job duties require such access; who have successfully completed a background check and any applicable security clearance; and who have been selected, approved, and trained accordingly.

5. The M.O.S.A.I.C. will, in the event of a data security breach, consider notifying an individual about whom personal information was or is reasonably believed to have been compromised or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. Any 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 breach or any measures necessary to determine the scope of the breach and, if necessary, to restore the integrity of the system**.**

L. Information Retention and Destruction

1. The M.O.S.A.I.C. will ensure that all ISE-SAR information is reviewed for record retention (validation or purge) in accordance with the time period(s) specified by 28 CFR 23 and Texas state law for criminal intelligence information.

2. The M.O.S.A.I.C. will retain ISE-SAR information in the shared space for up to 180 days to permit the information to be validated or refuted, its credibility and value to be reassessed, and a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, or under active investigation) assigned so that a subsequent authorized user knows the status and purpose for the retention and will retain the information based on any retention period associated with the disposition label. At the end of the 180 days, the entry will be reviewed and a determination made whether it has sufficient value to justify its retention in the system or meets other M.O.S.A.I.C. criteria for purge.

3. When ISE-SAR information has no further value or meets the M.O.S.A.I.C.'s criteria for purge under L. 1., above, privacy field information, at a minimum, will be purged.

4. No notice will be provided when information is purged under L. 1. - 3., above.

M. Transparency, Accountability, and Enforcement

M.1. Information System Transparency

1. The M.O.S.A.I.C. will be open with the public in regard to SAR collection and ISE-SAR information policies and practices. The M.O.S.A.I.C. will make its NSI Privacy Policy available upon request and post it on the Dallas Police Department Web site at http://www.dallaspolice.net/dpdinfo/dpdinfo.html

2. The M.O.S.A.I.C.'s Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections relating to ISE-SAR information.

M.2. Accountability

1. The audit log of queries for ISE-SAR information will identify the user initiating the query.

2. The M.O.S.A.I.C. will have access to an audit trail of inquiries to and information disseminated from the shared spaces.

3. The M.O.S.A.I.C. will adopt and follow procedures and practices to evaluate the compliance of its authorized users with ISE-SAR information policy and applicable law. This will include periodic and random audits of logged access to the shared spaces in accordance with NSI policy. A record of the audits will be maintained by the Dallas Police Department.

4. M.O.S.A.I.C. personnel shall report violations or suspected violations of the M.O.S.A.I.C.'s NSI privacy policy to the M.O.S.A.I.C.'s Privacy Officer.

5. The M.O.S.A.I.C. will conduct periodic audit and inspection of the information contained in its ISE-SAR shared space. The audit will be conducted by M.O.S.A.I.C. staff or an independent auditor, as provided by NSI policy. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the ISE-SAR information maintained by the M.O.S.A.I.C. in the shared space and any related documentation.

6. The M.O.S.A.I.C.'s appointed and trained Privacy Officer will periodically review the M.O.S.A.I.C.'s NSI Privacy and CR/CL Policy and the M.O.S.A.I.C. will make appropriate changes in response to changes in applicable law or policy determinations.

M.3. Enforcement

1. The M.O.S.A.I.C. reserves the right to restrict the qualifications and number of user agencies and authorized user agency personnel that it certifies for access to ISE-SAR information and to suspend or withhold service to any of its user agencies or authorized user agency personnel violating this privacy policy. The M.O.S.A.I.C. further reserves the right to deny access or participation in the NSI to users that fail to comply with the applicable restrictions and limitations of the M.O.S.A.I.C.'s privacy policy.

N. Training

1. The following individuals will participate in training programs regarding implementation of and adherence to this privacy, civil rights, and civil liberties policy:
   - All assigned personnel of the M.O.S.A.I.C.
   - Personnel providing information technology services to the M.O.S.A.I.C.
   - Staff in other public agencies or private contractors, as appropriate, providing SAR and ISE-SAR information technology or related services to the M.O.S.A.I.C.
   - Source agency personnel providing organizational processing services for SAR information submitted to the M.O.S.A.I.C.

2. The M.O.S.A.I.C.'s privacy policy training program will cover:
   - Purposes of the NSI Privacy and CR/CL Policy.
   - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of SAR and ISE-SAR information maintained or submitted by the M.O.S.A.I.C. to the shared space.
   - How to implement the policy in the day-to-day work of a participating agency.
   - The impact of improper activities associated with violations of the policy.
   - Mechanisms for reporting violations of the policy.
   - The possible penalties for policy violations, including transfer, dismissal, and criminal liability, if any.

Appendix A—Terms and Definitions

The following is a list of primary terms and definitions used throughout this 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. Data access is usually specified as read-only 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.

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

Agency—Agency refers to the **M.O.S.A.I.C.** and all agencies that access, contribute, and share information in the M.O.S.A.I.C.'s ISE-SAR information system.

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 (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

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

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.

Data—Data refers to elements of information.

Disclosure—Disclosure is 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.

Fusion Center—A fusion center is 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 their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

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

Information—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 four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

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.

ISE-SAR—An ISE-SAR is a suspicious activity report (SAR) 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)— An ISE-SAR IEPD is 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 associated 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.

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

M.O.S.A.I.C. – The Dallas Police Department Metro Operations Support and Analytical Intelligence Center

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.

Participating Agencies—Participating agencies, for purposes of the EE NSI, include source (the agency or entity that originates SAR [and, when authorized, ISE-SAR] information), submitting (which is the agency or entity posting ISE-SAR information to the shared space), and user (which is 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.

Personal Information—Personal information can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

Privacy—Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the right 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—Privacy fields are 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 personal information that it gathers and

uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, disclosure, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—This is a process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—For the non-intelligence 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 state, local, and tribal governments, the protections derived from applicable state and tribal constitutions and state, local, and tribal laws, ordinances, and codes. 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, or other similar instrument should be covered.

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/center's information.
- Media organizations.
- 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, which assist the agency/center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Record—Record refers to 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.

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 counter-terrorism activity.

Role-Based Access—Role-based access is a type of access that uses roles to determine 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 business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Shared Space—Shared space is a networked data and information repository which is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

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

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 information technology 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.

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

Suspicious Activity—Suspicious activity is defined as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity may, depending on the circumstances, include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (SARs)—SARs record the observation and documentation of a suspicious activity. 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 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 the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), terrorism information is all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials 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; or (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 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 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 should not technically be cited or referenced as a fourth category of information in the ISE.

Tips and Leads Information or Data—Tips and leads information or data is an uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads may also be referred to as suspicious incident reports (SIRs) and/or field interview reports (FIRs). A SAR is one type or subcategory of tips and leads. Tips and leads information does not include incidents that do not have an offense or possible offense attached, criminal history records, or Computer Aided Dispatch (CAD) data.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, anonymous or confidential sources, or a law enforcement investigation. This information has some level of suspicion attached to it, but without further inquiry or analysis, it is unknown whether or to what extent the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on whether time and resources are available to determine its meaning.

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

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

Appendix B -- Relevant State and Federal Laws

28 CFR Part 23; the principle of need to know, right to know.

The Texas Crime Information Center

The National Crime Information Center compliant

Criminal Justice Information Systems compliant

Texas Government Code 411.083 Dissemination of Criminal History Record Information

Texas Government Code 411.084 Use of Criminal History Record Information

Texas Government Codes 411.085 Unauthorized Obtaining, Use, or Disclosure of Criminal History Record Information; Penalty

Texas Government Code, Chapter 552, Public Information Act

Code of Federal Regulations, Title 28—Judicial Administration, Chapter I –Department of Justice, part 20 –Criminal Justice Systems, Subpart A – General Provisions