



Mississippi Analysis and Information Center

Privacy Policy

A. Purpose Statement

The Mississippi Analysis and Information Center (MSAIC) was authorized by Governor Haley Barbour on August 28, 2009, by Executive Order 1023, by emphasizing intelligence coordination between federal, state, local, tribal, and private sector organizations in order to prevent potential terrorist attacks and aid in response to attacks as well as respond to organized criminal activity. The mission of the MSAIC is to collect, evaluate, analyze and disseminate information and intelligence data regarding criminal and terrorist activity to federal, state, local and tribal law enforcement agencies, other Fusion Centers, and the public and private entities as appropriate, while following the Fair Information Practices to ensure the rights and privacy of citizens.

MSAIC's Privacy Policy applies to all individuals and organizations. Information shared in the ISE will be labeled and will be provided with the enhanced protections. The purpose of MSAIC's Privacy Policy is to ensure that MSAIC personnel with direct access to MSAIC information comply with federal, state, local and tribal laws, MSAIC's policies and procedures (See Appendix A., terms and definitions), and assists its authorized users in:

- Increasing public safety and improving national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the threat and risk of damage to real or personal property.
- Protecting individual privacy, civil rights, civil liberties, and other protected interests.
- Protecting the integrity of criminal investigations, criminal intelligence, and justice system processes and information.
- Minimizing reluctance of individuals or groups to use or cooperate with the justice system.

- Supporting the role of the justice system in society.
- Promoting governmental legitimacy and accountability.
- Not unduly burdening the ongoing business of the justice system.
- Making the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legal Compliance

All MSAIC personnel, Mississippi Department of Public Safety (MDPS), and Agency Representatives who provide information technology services to the MSAIC, and private contractors with direct access to MSAIC information will comply with the MSAIC's privacy policy concerning the information the MSAIC collects, receives, maintains, archives, accesses, or discloses to MSAIC personnel, governmental agencies, including the Information Sharing Environment (ISE), participating agencies, and participating justice and public safety agencies, as well as to private contractors and the general public.

The MSAIC will provide a printed copy of this policy to all personnel who are assigned to the MSAIC and have direct access to MSAIC information 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 MSAIC personnel with direct access to MSAIC information, Mississippi Department of Public Safety, and Agency Representatives and private contractors with access to MSAIC information and who provide information technology services to the MSAIC shall comply with applicable laws protecting privacy, civil rights, and civil liberties.

The MSAIC's internal operating policies are in compliance with applicable laws protecting privacy, civil rights, and civil liberties.

The MSAIC's authority for the collection, use, analysis, and retention/destruction of intelligence and non-intelligence information are cited in applicable constitutional provisions, 28 Code of Federal Regulations (CFR) Part 23 and in the following Mississippi Statutes; Mississippi Public Records Act of 1983 and Mississippi State Code 25-61-12.

C. Governance and Oversight

The Mississippi Office of Homeland Security was directed to create a Governance Board for MSAIC to provide strategic direction, ensure objectives are achieved, risks are managed appropriately, and resources are used responsibly. A Board of Directors representing significant participants in the MSAIC was also established, and meets regularly to provide input due to the collaborative nature of the MSAIC. Primary responsibility for the operation of the MSAIC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the Director of the MSAIC.

The Governance Board directed the MSAIC to develop a Privacy Policy. The Governance Board ensures that privacy and civil rights are protected within the provisions of this policy and within the MSAIC's information collection, retention, and dissemination processes and procedures. The Governance Board has mandated that the policy be reviewed and updated as appropriate.

The MSAIC has a 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 Information Sharing Environment program, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies.

The Privacy Officer is responsible for the direct oversight of the privacy policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information and thus is responsible for notifying the Director of the MSAIC regarding noncompliance issues.

D. Definitions

Primary terms and definitions used in the MSAIC Privacy Policy are located in Appendix A., page 17.

E. Information

The MSAIC's Watch Center serves as the focal point for the receipt, and dissemination of, criminal and terrorism activity information. The receipt and dissemination of information is recorded and maintained in the Watch Center's Call Log Information Sheet. All information sought and collected is noted in the Watch Center's Call Log Information Sheet. MSAIC's information is received from and disseminated to local, state, federal and tribal law enforcement, the public, and to private entities as appropriate. The Watch Center also supports emergency operations centers which coordinate Mississippi's response to significant man-made and natural disaster incidents.

The MSAIC will seek, view and/or retain information that:

- Is based on a criminal predicate or threat to public safety; or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that 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 of 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.

All MSAIC information will be sought, retained, shared, or disclosed under the appropriate policy provisions.

The MSAIC may retain information that is based on a level of suspicion that is less than reasonable suspicion, such as tips and leads and Suspicious Activity Reports (SAR) information. Tips and leads and SAR information will be labeled separately from other information.

The MSAIC 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 noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

The MSAIC personnel will, upon receipt of information, evaluate the information to determine its nature, usability, and quality. Personnel will assign labels to the information to reflect the assessment, and to ensure the proper segregation of information such as;

- Whether the information is based upon a standard of reasonable suspicion of criminal activity;
- Whether the information consists of tips and leads data or suspicious activity reports;
- The nature of the source as it affects veracity (for example, anonymous tips, trained interviewer or investigator, public record, private sector); and
- The validity of the content (for example, verified, partially verified, unverified, or unable to verify).

At the time a decision is made to retain information, it will be labeled pursuant to applicable limitations on access and sensitivity of disclosure to:

- Protect confidential sources and law enforcement undercover techniques and methods;
- Not interfere with or compromise pending criminal or terrorism investigations;
- Protect an individual's right of privacy, civil rights, and civil liberties; and
- Provide legally required protection based on the individual's status such as a juvenile.

The classification of existing information will be re-evaluated 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; for example, the information becomes part of court proceedings for which there are different public access laws.

MSAIC personnel will be required to adhere to specific practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and SARs information, once the guidelines are finalized and issued to Fusion Centers.

The MSAIC will incorporate 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 the information, as well as constitutional rights, including personal privacy and other civil liberties, and civil rights.

For purposes of sharing information in the Information Sharing Environment, the MSAIC will identify and label all terrorism related information and provide the enhanced privacy protections for such information required by this policy.

The MSAIC will attach specific labels that will be used, assessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

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

- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect an individual's right of privacy or their civil rights and civil liberties.
- Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

The MSAIC will keep a record of the source of all information retained.

The MSAIC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:

- The name of the originating center, department or agency, component, and subcomponent.
- The name of the center's justice information 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.

F. Acquiring and Receiving Information

Information gathering and investigative techniques used by the MSAIC and participating agencies are in compliance with and will adhere to regulations and guidelines, including, but not limited to:

- 28 CFR Part 23 regarding criminal intelligence information.
- Organization for Economic Co-operation and Development's Fair Information Practices (under certain circumstances, there may be exceptions to the Fair Information Practices, based, for example on authorities paralleling those provided in the Federal Privacy Act; state, local and tribal laws; or MSAIC policy.)
- Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP).
- Applicable constitutional provisions, State of Mississippi Executive Order 1023 and Mississippi Statutes which include and in the following Mississippi Statutes; Mississippi Public Records Act of 1983 and Mississippi State Code 25-61-12.

The MSAIC'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 MSAIC'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 MSAIC will be the least intrusive means necessary in the particular circumstance to gather information it is authorized to seek or retain.

MSAIC 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. Center personnel will:

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.
- Store the information using the same storage method used for data which rises to the level of reasonable suspicion and which 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 standard 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 long enough to work an un-validated tip, lead, or SAR information to determine its credibility and value or assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the center’s physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion. External agencies that receive and share information with the MSAIC are governed by the laws and rules governing those individual agencies as well as by applicable federal and state laws.

External agencies that receive and share information with the MSAIC are governed by the laws and rules governing those individual agencies as well as by applicable federal and state laws.

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

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

- An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
- An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

G. Information Quality Assurance

The MSAIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information. The MSAIC will make every reasonable effort to ensure that the information is accurate, current and complete, including the relevant context in which it was sought or received; and the information is merged about the same individual or organization only after utilizing the applicable standards.

At the time of retention in the system, the information will be accessed and labeled regarding its level of quality (accuracy, current, verifiable, and reliable).

The MSAIC investigates, in a timely manner, alleged errors and deficiencies and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

The labeling of retained information will be re-evaluated when new information is gathered that has an impact on the confidence (validity and reliability) in previously retained information.

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

Originating agencies external to the MSAIC are responsible for the quality and accuracy of the data accessed by or provided to the MSAIC. The MSAIC will advise the appropriate contact person in the originating agency, in writing, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

The MSAIC 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 MSAIC; for example, when the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the individual may be affected.

H. Collation and Analysis

Information acquired or received by the MSAIC, or accessed from other sources will be analyzed only 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 E, Information.

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

- Further crime prevention (including terrorism), law enforcement, force deployment, or prosecution objectives and priorities established by the MSAIC, 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 or terrorist activities.

I. Merging Records

Records about an individual or organization from two or more sources will not be merged 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 higher accuracy of match.

The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

If the matching requirements are not fully met, but there is an identified partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

J. Sharing and Disclosure

Access to MSAIC information:

- The Director of the MSAIC, and/or administrator(s) designated by the Director, shall establish requirements and record all personnel as to their access authority and permission to access MSAIC's information;
- Permissions regarding viewing, adding, editing and printing of MSAIC information is controlled by MSAIC's administrator(s) on all MSAIC's information;
- All MSAIC personnel, with approval from the Director, or his designee, may disclose MSAIC information may be shared with individuals or organizations with a right to know/need to know for a legitimate law enforcement/terrorism purpose, consistent with applicable law;
- An audit trail shall be maintained regarding access to, and disclosure of, MSAIC information.

The MSAIC will adhere to the national standards for the SAR process. This will include the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the Information Sharing Environment Functional Standard SAR.

Access to, or disclosure of, records retained by the MSAIC will be provided only to persons within the MSAIC or in other governmental agencies who are authorized to have access, and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes, and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. The Watch Center Call Log records all disseminations of information by MSAIC personnel.

Agencies external to the MSAIC may not disseminate MSAIC information received from MSAIC without approval from the originator of the information.

Records retained by the MSAIC may be accessed or disseminated to those responsible for public protection, public safety, or public health only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. As stated, the Watch Center Call Log records all disseminations.

Information gathered and records retained by the MSAIC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access, and only for those users and purposes specified in the law. The Watch Center Call Log which notes receipt and dissemination of this type of information will be kept a minimum of five years for this type of request. Thus requests and disseminations for specific purposes are recorded and maintained.

Information gathered and records retained by the MSAIC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record pursuant to

Mississippi Statute; Mississippi Public Records Act of 1983 and Mississippi State Code 25-61-12 or otherwise appropriate for release to further the MSAIC 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 MSAIC for this type of information or when there is a legitimate need. Requests of this nature are recorded in the Watch Center Call Log. The request and any information disclosed are recorded in the Watch Center Call Log.

Information gathered and records retained by the MSAIC will not be:

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

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

- Records required to be kept confidential by law are exempted from disclosure requirements under Mississippi Statute, Mississippi State Code 25-61-12.
- Investigatory records of law enforcement agencies are exempted from disclosure requirements under Mississippi Statutes, Mississippi State Code 25-61-12 (D). However, certain law enforcement records must be made available for inspection and copying under Mississippi Statute, Mississippi State Code 25-61-5.
- 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 Mississippi Statutes Mississippi State Code 25-61-11. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under Mississippi Statutes, Mississippi State Code 7-1-19 & 7-1-21.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission.
- A violation of an authorized nondisclosure agreement.
- Information that meets the definition of “classified information” as that term is defined in the National Security Act, Public Law 235, Section 606.

The MSAIC 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.

K. Redress

K.1 Disclosure

Requests for disclosure of MSAIC records by the public will be handled according to established procedures under Mississippi Public Records Act of 1983 and Mississippi State Code 25-61-12. The MSAIC'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 to an individual.

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

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution Mississippi State Code 25-61-12;
- Disclosure would endanger the health or safety of an individual, organization, or community Mississippi State Code 25-61-12;
- The information is in a criminal intelligence system Mississippi State Code 25-61-12;
- Disclosure to the individual is exempt or prohibited by applicable U.S. Code, state statute or administrative rule;
- The information source does not reside with the MSAIC Mississippi State Code 25-61-12;or
- The MSAIC did not originate or does not have a right to disclose the information;
- Other authorized basis for denial;

K.2 Complaints and Corrections

If an individual has complaints or objections to the accuracy or completeness of information about him or her originating from MSAIC information, the MSAIC will inform the individual of the procedure for submitting complaints or objections (if not properly communicated) or requesting corrections. The contact information of the MSAIC's Privacy Officer will be posted on the Mississippi Office of Homeland Security's (MOHS) website – www.homelandsecurity.ms.gov . The Privacy Officer can be contacted at MSAIC ATTN: Privacy Officer 1 MEMA Drive Pearl, MS 39208. If an individual's complaint or objection cannot be resolved after review at the MSAIC, the individual may request a review of that decision, by the Mississippi Department of Public Safety is the host agency for the MSAIC. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

If an individual has complaints or objections to the accuracy or completeness of information about him or her that originates with another agency, the MSAIC will notify the source agency of the complaint or request for correction, and coordinate with the source agency to ensure that the individual is provided with applicable complaint submission or corrections procedures. A record will be kept of all such complaints and request for corrections, and the resulting action taken, if any.

The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the MSAIC, or the originating agency.

If an individual has complaints or objections to the accuracy or completeness of MSAIC/ISE-SAR information allegedly held by the MSAIC that has allegedly resulted in specific, demonstrable harm to such individual, the MSAIC will inform the individual of the procedure for submitting complaints or requesting corrections (if not properly communicated). The MSAIC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of any MSAIC/ISE-SAR information in privacy fields that identifies the individual. However, any personal information will be reviewed and confirmed or corrected in, or deleted from MSAIC/ISE-SAR shared space within 45 days if the information is determined to be erroneous, included incorrectly merged information, or is out of date. If there is no resolution within 45 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept of all complaints and requests for corrections, and the resulting actions, if any.

K.3 Appeals

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

L. Security Safeguards

The MSAIC's Fusion Center Security Liaison Officer is designated and trained to serve as the MSAIC's Security Officer.

The MSAIC is located within the headquarters of the Mississippi Emergency Management (MEMA), which is a secure facility, thus protected from external intrusion. The MSAIC's office space is only accessible to MSAIC personnel and other MOHS personnel that have been issued an access card for the MSAIC. The MSAIC will utilize secure internal and external safeguards against network intrusions. Access to MSAIC systems from outside the facility will be allowed only over secure networks. The MSAIC's information system is an Mississippi Department of Public Safety (MDPS) system and thus maintained by them. All MDPS systems, to include the MSAIC system, are required to complete an annual security risk assessment. The purpose of this annual assessment is to identify vulnerabilities. All MSAIC information systems are required to

be compliant with ISO/IE 17799 standards, National Institute of Standards and Technology Special Publications 800-30 standards, and PCI DSS standards.

The MSAIC will label tips and leads, SAR information, and the Information Sharing Environment protected information, and they will reside in a repository system that is the same as, or similar to, the system that secures data rising to the level of reasonable suspicion.

The MSAIC 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.

Direct access to MSAIC's information will be granted only to MSAIC personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

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

The MSAIC utilizes the Watch Center Call Log to record requested and disseminated information.

To prevent public records disclosure, risk and vulnerability assessments are stored in the Automated Critical Asset Management System database, a separate system, and will not be stored with publicly available data.

M. Information Retention and Destruction

All MSAIC generated information (intelligence/non-intelligence) and/or information (intelligence/non-intelligence) furnished to MSAIC, some of which may be for dissemination, will be reviewed for record retention (validation or purge) at least every five years.

The MSAIC will delete information, or return it to the source, as required in Mississippi Statutes, or as specified in 28 CFR Part 23.

The MSAIC's authority for the collection, use, analysis, and retention/destruction of intelligence and non-intelligence information are cited in applicable constitutional provisions, 28 Code of Federal Regulations (CFR) Part 23 and as authorized by Governor Haley Barbour on August 28, 2009, by Executive Order 1023, by emphasizing intelligence coordination between federal, state, local, tribal, and private sector organizations in order to prevent potential terrorist attacks and aid in response to attacks as well as respond to organized criminal activity.

All MSAIC information will be periodically reviewed for relevancy and importance. Information which has been determined to be invalid, untrue, obsolete, no longer useful because the purpose for which it was collected has been satisfied or no longer exists will be purged, destroyed, and deleted from the system. The MSAIC is not required by law or regulation to notify source

agencies of the purge of information or intelligence from MSAIC databases. Source agencies will not be notified when information they have submitted is due for purge from MSAIC information or intelligence databases. Purged dates will be tracked in electronic databases based on the date of record entry into the database.

N. Accountability and Enforcement

N.1 Information System Transparency

The MSAIC will be open with the public in regard to information and intelligence collection practices. The MSAIC's Privacy Policy will be provided to the public upon request. Information for the existence and obtaining/requesting a copy of the Privacy Policy will be posted on the website - www.homelandsecurity.ms.gov .

The MSAIC's Privacy Officer will be responsible for receiving inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s). The contact information of the MSAIC's Privacy Officer will be posted on the Mississippi Office of Homeland Security's website – www.homelandsecurity.ms.gov . The Privacy Officer can be contacted at MSAIC ATTN: Privacy Officer, 1 MEMA Drive Pearl, MS 39208. The MSAIC's Privacy Officer will report all inquiries and complaints to MDPS's Legal Department. The Legal Department will direct the handling and response to inquiries/complaints.

N.2 Accountability

The Watch Center Call Log records queries, disseminations and other pertinent information. Accessing the Watch Center Call Log Information Sheet identifies the user in the MSAIC's audit system.

The MSAIC, through entries in the Watch Center Call Log, maintains information of accessed, requested, or disseminated information. The Watch Center Call Log Information Sheet will be kept for five years to identify who requested information and to whom information was disseminated. The MSAIC's audit system records access to the Watch Center Call Log Information Sheet.

The MSAIC will provide a copy of this policy to all MSAIC personnel and will require written acknowledgement of receipt of this policy and the provisions it contains.

The MSAIC's Privacy Officer will periodically conduct random audits annually to ensure and evaluate the compliance of users. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least annually and a record of the audits will be maintained by the Privacy Officer of the center.

The MSAIC's personnel, or other personnel participating with the MSAIC, shall report violations or suspected violations of MSAIC policies relating to protected information to the MSAIC's Privacy Officer and/or the Director.

The Privacy Officer will conduct random audits during a one year time frame of the Watch Center's information.

The MSAIC's Governance Board, guided by the trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy at least annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

The MSAIC will notify an individual about whom sensitive, personally identifiable information was, or is reasonably believed to have been, breached or obtained by an unauthorized person and access to which threatens physical, reputational, 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.

N.3 Enforcement

If an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification or disclosure of information, the Director of the MSAIC will:

- Notify in writing the chief executive of the employing agency of the violation and noncompliance of his or her employee.
- Initiate an investigation, criminal if appropriate.
- As the MSAIC is a multi-agency effort, MSAIC's Director will work with each agency regarding their personnel policies for appropriate sanctions that do not rise to the criminal matter.
- Agencies must take action to correct such violations and provide an assurance in writing to the MSAIC Director that corrective action has been taken.
- The failure to remedy violations may result in suspension or termination of access by the employee to MSAIC information.
- The MSAIC reserves the right to restrict the qualifications and number of personnel having direct access to MSAIC information, and to suspend or withhold service to any participating agency user who fails to comply with the applicable restrictions and limitations of the MSAIC's Privacy Policy.

O. Training

The MSAIC will require annual training for the following individuals regarding implementation of and adherence to the Privacy Policy:

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

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

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

Destruction of Purged Material

- A. Purged documents and materials will be destroyed either by a supervised burning or shredding process, or by some other method which will totally destroy the material as per 28 CFR Part 23.

Appendix A – Definitions

The following are the primary terms and definitions used in this privacy policy document:

Definitions

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. 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.

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 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—The Mississippi Analysis and Information Center and all agencies that access, contribute, and share information in the Mississippi Analysis and Information Center's justice information system.

Audit Trail—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—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—Refers to the Mississippi Analysis and Information Center and all participating state agencies of the Mississippi Analysis and Information Center.

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. 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” is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, 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—The protection of information assets through the use of technology, processes, and training.

Confidentiality—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 used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal Intelligence Information—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 activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

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

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

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

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

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

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

Fair Information Practices – The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development’s Guidelines on the Protection of Privacy and Trans-border 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.

The eight FIPs are:

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

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

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

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

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

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

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information.

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.

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

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

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

Law—As used by this policy, law includes any local, state, or federal constitution, 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.

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

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

Logs—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 data. See also Audit Trail.

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

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

Need to Know— 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.

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

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

Participating Agency—An organizational entity that is authorized to access or receive and use center information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

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

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information.

Personally Identifiable Information—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, Integrated Automated Fingerprint Identification System [IAFIS] 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 United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation

directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, “persons” means United States citizens and lawful permanent residents.

Privacy—Refers to individuals’ interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the center will adhere to those legal requirements and center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the center, the individual, and the public; and promotes public trust.

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

Protected Information—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. While not within the definition established by the ISE Privacy Guidelines, protection may be extended to other individuals and organizations by internal federal agency policy or regulation.

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.

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

Public—Public includes:

Any person and any for-profit or nonprofit entity, organization, or association.

Any governmental entity for which there is no • existing specific law authorizing access to the 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 center or participating agency.

Public does not include:

Employees of the center or participating agency.

People or entities, private or governmental, who assist the center in the operation of the justice information system.

Public agencies whose authority to access information gathered and retained by the center is specified in law.

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

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

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

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

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also

have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

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

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:

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 is probably the most common meaning in the IT industry.

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—including 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.

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

Suspicious Activity Report (SAR)—Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it 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), 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 the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of “terrorism information,” as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute “terrorism information”: (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include intelligence information.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of “terrorism information” by P.L. 110-53.

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. 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 falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

User—An individual representing a participating agency who is authorized to access or receive and use a center’s information and intelligence.