Washington State Fusion Center
Privacy Policy

Purpose Statement

The purpose of the Washington State Fusion Center (WSFC) Privacy Policy is to ensure that the collection, evaluation, analysis and dissemination of information and intelligence data regarding criminal activity is conducted in a manner that protects public safety while protecting civil rights, civil liberties and personal privacy. This policy has the express purpose of fulfilling that mission by ensuring strict adherence to all applicable federal and state constitutional rights, statutory, and regulatory protections while:

- 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; and
- Making the most effective use of public resources allocated to public safety agencies.

Policy Applicability and Legal Compliance

1. The WSFC will adopt a Concept of Operations and Standard Operating Procedures that are consistent with the provisions of this privacy policy, as well as all applicable state and federal constitutional rights and statutes and regulations, including 28 CFR Part 23.

2. All personnel assigned to the WSFC, including private contractors and authorized participating agencies will comply with the WSFC's privacy policy while carrying out WSFC responsibilities at the direction of the WSFC and its representatives, or otherwise acting within the scope of their assigned WSFC duties. Nothing in this policy is, however, meant to preempt superseding federal or state laws, regulations, or constitutional provisions.

3. The WSFC will make this policy available on-line to personnel and authorized users and will provide a printed copy of this policy to all WSFC personnel, who will be required to sign both a written acknowledgement of receipt of this policy, as well as a written agreement to comply with the privacy policy.

4. It is the policy of WSFC, where relevant and appropriate, to provide the enhanced protections of the Information Sharing Environment (ISE) for terrorism-related information to all personal identifiable information shared by WSFC with authorized participating agencies.

Governance and Oversight

1. The WSFC Executive Board is responsible for approving WSFC policies and procedures and ensuring that audit and oversight mechanisms are in place to ensure compliance. The Director of the WSFC is responsible for approving an Interim Privacy Policy until the Executive Board can approve a final policy. The Director is also responsible for the day-to-day operations of the WSFC, including enforcement of this privacy policy. The Director will appoint a designated and trained internal Privacy and Civil Liberties Officer to monitor compliance with this policy and act as a resource. This person will also act as the liaison for the Information Sharing Environment.

2. The WSFC Executive Board will establish a privacy oversight mechanism to review and make recommendations regarding WSFC privacy policy and procedures to ensure that appropriate revisions are made in response to changes in technology, policy, or law, and to oversee a minimum of an annual audit of WSFC operations to determine compliance with this policy.

3. Personnel, contractors and others who fail to abide by provisions of this policy applicable to them may be denied access to information sharing mechanisms of the WSFC or other appropriate sanction as determined by the WSFC Executive Board, including potential termination of participation with the WSFC.

Information Collection, Retention and Dissemination Standards

1. The WSFC will only collect, analyze, retain or disseminate information that was lawfully obtained and is relevant to the investigation and prosecution of suspected criminal activity, threats to public safety or other legitimate criminal justice purpose. For purposes of this policy, "information" includes any information or intelligence "about an identifiable individual or organization that the WSFC may legally obtain, review, retain, etc., such as suspicious activity reports (SARs) and other tips and leads information, criminal histories, incident reports, public records, etc." See Appendix C for SAR Guidelines that the WSFC will follow for this type of information.

2. The WSFC will not seek, retain or disseminate any information about individuals or organizations solely on the basis of their race, ethnicity, gender, age, sexual orientation or disability. This protection also extends to religious or political activities and beliefs. Since government actions can unintentionally inhibit the exercise of state and federal constitutional rights, this policy further specifically prohibits the collection, retention or dissemination of personal identifying information (PII) about an individual's non-criminal participation in protected First Amendment activities such as speech, assembly and petition which may take various forms to include protests, rallies, etc., without a legitimate law enforcement purpose meeting the standards and procedures of this policy.

3. Any criminal information related to protected First Amendment activities shall be first reviewed by the Privacy and Civil Liberties Officer and then specifically approved by the WSFC Director prior to retention or dissemination. In addition to the applying the criminal standard, the review and approval shall ensure that any misdemeanor criminal conduct alleged has a legitimate law enforcement purpose and is relevant to the core responsibilities of the WSFC.

4. When the decision to retain information is made, it will be labeled, stored and disseminated in a manner that:

   - Protects the right of privacy and civil liberties
   - Protects confidential sources and methods
   - Provides all legally required protections

   Information will be assessed upon receipt to determine its nature, usability, and quality and labeled to indicate to the user the category of information, the nature of the source, and confidence levels, where appropriate. The labeling of retained information will be reevaluated when new information is collected that has an impact on the confidence in previously retained information.

5. All personal identifiable information collected by WSFC and shared through the ISE, shall include, where relevant and appropriate, the name of the originating agency, the information system from which the information is provided, the date the information was collected, and the title and contact information for the person in the originating agency to whom inquiries should be directed.

6. All personal identifiable information with access restrictions will be so labeled when it is disseminated to reflect limitations on access and sensitivity of disclosure. Those limitations will be updated when the WSFC receives new information that impacts those access restrictions or there is a change in the use of the information affecting access or disclosure limitations.

7. Information gathering and investigative techniques used by the WSFC and information originating agencies shall be in compliance with and will adhere to applicable constitutional provisions, statutes and regulations. Intelligence information shall be collected, stored and disseminated in compliance with 28 CFR Part 23 (Appendix A), and the LEIU Criminal Intelligence File Guidelines (Appendix B), including the Third Party Rule, as well as all applicable federal and state constitutional provisions.

Information Quality Assurance

1. The WSFC will make every reasonable effort to ensure that, prior to retaining or disseminating information, the information is accurate and complete, and includes the context in which the information was received. This will include labeling

information to identify, where relevant and appropriate, its source and level of quality, including confidence in the information (source reliability and content validity), accuracy, completeness, currency, and whether it has been verified.

2. The WSFC will investigate and correct or delete, in a timely manner, any alleged errors and deficiencies in the information the fusion center has retained or disseminated, whether by internal discovery or external complaint of error. If the WSFC discovers that information it has received from an originating agency is inaccurate or otherwise unreliable, it will notify the originating agency in writing, including electronic notification. This will include written (electronic) notification to any individual or entity that the WSFC knows has received the incorrect information. To facilitate these notifications, the WSFC will develop a computer system that tracks the dissemination of information and intelligence and any corrections (including related new information) or deletions.

3. All criminal intelligence information will be electronically marked with its purge date upon entry into a criminal intelligence database and validated for retention purposes or purged at least every five years. Information and intelligence that is no longer relevant, including criminal intelligence information no longer eligible to be retained under 28 CFR Part 23, will be electronically purged, returned to the originating agency as appropriate, or otherwise archived as required by law. Source agencies will not be notified of pending purge dates.

4. 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 a higher accuracy of match If the information is insufficient to allow merging of the record, 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.

5. Records will be provided to requestors, unless exempt from disclosure under chapter 42.56 RCW Washington Public Records Act. When information is exempt from disclosure and an individual or group has a complaint or other objection to the accuracy of information regarding that person or group, the WSFC will acknowledge the complaint and: (a) if the information originates from the WSFC, the WSFC will investigate the complaint and either conform the information, correct it, or remove it from an information database; or (b) if the information does not originate from the WSFC, the complaint will be referred to the source agency for investigation. A record of all such requests, and any confirmation or correction/removal action taken, will be maintained by the WSFC. Pending investigation and resolution, the information complained about will not be disseminated by the WSFC.

6. The WSFC Director will be responsible to ensure that all complaints about information originating from the WSFC are fully investigated, appropriate action is taken in response to the investigation, and notification of resolution is made to the complainant. Such notification will include the procedure to appeal the Director's determination, as provided by the Washington Public Records Law.

Information Security

1. Credentialed, role-based criteria are crucial for information security and privacy protections. Access limitations, along with an inquiry log and audit trail maintained by WSFC for WSFC databases, will identify and limit:

   - The authorized user making an inquiry, the subject of the inquiry, and the information that the user has accessed;
   - Whether the authorized user can enter, change, delete or print information or took any of these actions; and
   - To whom information can be disseminated and under what circumstances.

   Only qualified individuals with the appropriate credentials and training will analyze information acquired or accessed by the center.

   These restrictions will be reevaluated whenever the WSFC receives additional information which merits a change in information restrictions, such as a national security classification.

2. Access to or disclosure of records collected or retained by the WSFC will be provided only to persons who are authorized to have such access in accordance with all applicable federal and state laws, and in furtherance of legitimate public safety purposes. All WSFC personnel, including contractors will undergo a full background investigation in addition to a security clearance investigation for those individuals having access to classified information.

3. Any information disseminated by the WSFC will contain dissemination restriction language appropriate for the particular type of material, such as "law enforcement sensitive," and "third-party" rule restrictions.

4. The WSFC Director shall appoint a security officer. The Security Officer shall receive appropriate training and shall work in concert with the FBI security manager to ensure compliance with information security procedures. These security procedures will include:

   - Secure internal and external safeguards against network intrusions;
   - Information will be stored so that it cannot be modified, accessed, destroyed or purged except by authorized personnel with the appropriate background investigations and security clearances; and
   - Appropriate physical security safeguards are in place to protect information.

5. Risk and Vulnerability Assessments will be stored separately from publicly available data.

6. Unless legal or security restrictions prohibit it, or unless it would compromise a legitimate law enforcement purpose, such as an ongoing investigation, source or method, etc., (a) the WSFC will follow RCW 42.56.590 in the event of a data security breach; and (b) the WSFC will protect sensitive government records and private information consistent with chapter 42.56 RCW,, the Washington Public Records Act.

Accountability and Enforcement

1. The public has a right to know the information and privacy safeguards of the WSFC. The WSFC's privacy policy will be made available upon request and will be posted on a public web portal to be developed.

2. To enable oversight and enforcement of these provisions, the WSFC will implement a computerized record system that maintains an audit trail of all access and dissemination of WSFC records. This audit trail will be maintained a minimum of five years.

3. In addition to being provided a copy of this policy, all WSFC personnel will be required to participate in training regarding adhering to this policy. This training will include, at a minimum, the purpose of the policy, substance and intent of the provisions of the policy, impact of infractions, and possible penalties for violations. Personnel authorized to share personal identifiable information in the ISE shall receive specialized training regarding WSFC requirements and policies for the collection, disclosure and use of this information. User agencies, not the WSFC, are responsible for providing appropriate training, such as how to handle intelligence or law enforcement sensitive information, e.g., the Third Party Rule, to their personnel submitting information to WSFC or who have access to protected information disseminated by WSFC.

4. All personnel assigned to the WSFC have a duty to uphold the privacy and civil liberties protections in this policy, to cooperate with audits and reviews by oversight officials with responsibility for information sharing, and to report violations of WSFC policies related to protected information to the WSFC Privacy and Civil Liberties Officer, who shall serve as the initial receiving point for inquiries and complaints about privacy and civil liberties concerns, and who will receive reports of suspected or confirmed violations. The WSFC Director is responsible for ensuring adherence to this policy.

5. The WSFC Executive Board will ensure that an annual audit is conducted to review compliance with WSFC information systems requirements and the WSFC Privacy Policy. The panel will report its findings to the Executive Board along with any

recommendations for corrective action or policy modification. If suggestions for policy modification are approved, the Policy will be updated annually to reflect those suggestions and any other modification required in response to changes in applicable law, technology, or the purpose and use of information systems.

Appendix A – 28 CFR Part 23

See:
http://www.iir.com/28cfr/pdf/ExecOrder12291_28CFRPart23.pdf.

and
http://www.iir.com/28cfr/pdf/1993RevisionCommentary_28CFRPart23.pdf.

Appendix B- LEIU File Guidelines

See: http://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf.

Appendix C- SAR Guidelines

The WSFC will incorporate the gathering, processing, reporting, analyzing, and sharing of Suspicious Activity Reporting (SAR) 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. In addition to those protections, the following provisions uniquely apply to SAR information and are derived from the Program Manager's Office of the Information Sharing Environment (PM-ISE) regarding the National SAR Initiative operated under the auspices of that office.

Information Collection, Retention and Dissemination Standards

1. All WSFC personnel will receive training to recognize behaviors and other indicators of criminal activity related to terrorism that also includes training to avoid inappropriate behavior in violation of this policy such as racial, religious or ethnic profiling.

2. Upon receipt of SAR information from a source agency that has processed the information in accordance with WSFC criteria, designated WSFC personnel will:

    - Personally review and vet the SAR information and provide the two-step assessment set forth in the ISE-SAR Functional Standard to determine whether the information qualifies as an ISE-SAR (alternatively, WSFC personnel will confirm that such an assessment has been conducted by an authorized source agency).
    - Enter the information following Information Exchange Package Documentation (IEPD) standards and code conventions to the extent feasible.
    - Provide appropriate labels as required under #3 below.
    - Post the ISE-SAR to the FC's shared space.
    - Notify the source agency that the SAR has been identified as an ISE SAR and submitted to the shared space.

3. The WSFC will ensure that certain basic and special descriptive information is entered and electronically associated with ISE-SAR information, including:

    - The name of the source agency.
    - 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.

4. Information provided in the ISE-SAR shall indicate, to the maximum extent feasible and consistent with the *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0* (ISE-FS-200):

    - *The nature of the source*: anonymous tip, confidential source, trained interviewer or investigator, written statement (victim, witness, other), private sector, or other source.
    - Confidence, 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 by the source or submitting agency, 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 the source or submitting agency or validate it through their own investigation.

5. At the time a decision is made to post ISE-SAR information to the shared space, WSFC personnel will ensure that the ISE-SAR information is labeled, to the maximum extent feasible and consistent with the ISE-SAR FS, to reflect any limitations on disclosure based on sensitivity of disclosure (dissemination description code), in order to:

    - Protect an *individual's* right to 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.

6. The WSFC will share ISE-SAR information with authorized nonfusion center agencies and individuals only in accordance with established WSFC policy and procedure.

7. 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.

Information Quality Assurance

1. The WSFC will ensure that source agencies assume primary responsibility for the quality and accuracy of the SAR data collected by the WSFC. The WSFC will advise the appropriate contact person in the source agency in writing (this would include electronic notification) if SAR information received from the source agency is alleged, suspected, or found to be erroneous or deficient.

2. The WSFC will make every reasonable effort to ensure that SAR information collected and ISE-SAR information retained and posted to the shared space is derived from dependable and trustworthy source agencies 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 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 did not have authority to provide it to the WSFC or if the information is subject to an expungement order in a state or federal court that is enforceable under state law or policy.

7. The WSFC will provide written notice (this would include electronic notification) to the source agency that provided the SAR and 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 WSFC is corrected or removed from the shared space by the WSFC because it is erroneous or deficient such that the rights of an individual may be affected.

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 WSFC will adhere to the Functional Standard for the ISE-SAR process, including the use of the ISE-SAR IEPD reporting format, EE Initiative-approved data collection codes, and ISE-SAR information sharing and disclosure business rules.

3. ISE-SAR information retained by the WSFC and entered into the WSFC's shared space will be accessed by or disseminated only to persons within the WSFC 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***. Access and disclosure of personal information will be allowed to agencies and individual users only for legitimate law enforcement and public protection purposes and for the performance of official duties in accordance with law.

Appendix D- Definitions

The following is a list of primary terms and definitions used throughout the WSFC Interim Privacy Policy.

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

Agency—Agency refers to the WSFC and all agencies that access, contribute, and share information in the [name of agency]'s justice 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.

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.

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 RightsCthe 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.

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

Data—Inert symbols, signs, descriptions, or measures.

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

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

Electronically Notification—Notice that is provided 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.

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.

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.

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

Personal Identifiable Information—Personal identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to identify a unique individual.

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 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 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, dissemination, 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 nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. For state, local, and tribal governments, it includes 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; and
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

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

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

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

Retention—Refer to Storage.

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.

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.

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

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

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

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

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 include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Report (SAR)—Official documentation of a suspicious activity. At the federal level, there are two types of SAR information: 1) Information Sharing Environment SAR information that pertains to terrorism information; and 2) Banking Secrecy Act SAR information that pertains to suspicious banking activity and is required to be completed by financial institutions. 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, the state-designated fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of IRTPA, all information relating to (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.

Weapons of Mass Destruction (WMD) information is a defined sub-category of terrorism information.

Terrorism-Related Information—In accordance with 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 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.

Tips and Leads Information or Data—Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads may include suspicious incident report (SIR) information, suspicious activity report (SAR) information, and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data. Tips and leads information should 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 raises some suspicion but may be based on a level of suspicion that is less than "reasonable suspicion" and, without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.