WSIC Privacy Policy

Effective: June 1, 2013

Table of Contents

A. Intent

The Wisconsin Statewide Information Center (WSIC) is committed to the responsible and legal compilation and utilization of criminal investigative and criminal intelligence information and other information important to protecting the safety and security of the people, facilities and resources of the State of Wisconsin and the United States. All compilation, utilization and dissemination of personal data by WSIC participants and source agencies will conform to requirements of applicable state and federal laws, regulations and rules, and - to the greatest extent practicable - be consistent with Fair Information Practices.

The intent of this policy is to abide by all privacy, civil rights and civil liberties guidance issued as part of the Intelligence Reform and Terrorism Prevention Act of 2004, National Fusion Center Guidelines and the National SAR Initiative. All local, state, tribal and federal agencies providing suspicious activity reports (SAR) with a nexus to Wisconsin or participating with the Wisconsin Statewide Information Center (WSIC) by virtue of submitting, receiving or disseminating SAR information, criminal intelligence or criminal investigative information via WSIC, are required to adhere to the requirements of the Wisconsin Statewide Information Center Privacy Policy.

B. Background

A Fusion Center is a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend and respond to criminal and terrorist activity. WSIC is inclusive of and a component within the Wisconsin Department of Justice, Division of Criminal Investigation, located in Madison, Wisconsin. WSIC consists of federal agencies, state multi-disciplinary partners, local law enforcement, emergency service and criminal justice agencies. WSIC also engages in active outreach to private sector security entities. WSIC serves as the state's primary focal point for threat information sharing among federal, state, local and tribal law enforcement, emergency management, fire service, public health, corrections, military and private sector security partners for the state.

In order to deter, prevent, and mitigate criminal or terrorist threats while protecting the privacy and civil liberties of U.S. citizens, WSIC accomplishes the following mission essential tasks:

- Provides case support to law enforcement agencies for major criminal investigations;
- Gathers, receives, analyzes and disseminates intelligence at the national, state and local levels;
- Performs critical services for government and private sector partners;
- The Clearinghouse for Missing and Exploited Children and Adults;
- The AMBER Alert Program;
- The Wisconsin Crime Alert Network;
- Provides Training and Outreach;
- Threat Liaison Officer and Fusion Liaison Officer Programs;
- Continuing education for government and private sector partners; and
- Protects the civil liberties and privacy interests of United States persons throughout the intelligence process.

C. Purpose

The purpose of this privacy policy is to promote WSIC, source agency and user agency conduct that complies with federal, state, local and tribal laws, regulations, and policies applicable to information and intelligence collection, use and sharing, and assists them in:

- Ensuring individual privacy, civil rights, civil liberties, and other protected interests;
- Increasing public safety and national security while maintaining appropriate levels of operational transparency;
- 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.

D. Policy Applicability and Legal Compliance

All WSIC personnel, IT personnel, private contractors, and other authorized users will comply with applicable provisions of WSIC's privacy policy concerning the information the center gathers, receives, analyzes, and disseminates to center members, governmental agencies, and participating agencies, as well as to private contractors and the general public. This includes SAR information that source agencies collect and WSIC receives as well as ISE-SAR information identified, submitted to the shared space, and accessed by or disclosed to WSIC personnel. All WSIC personnel are required to sign a non-disclosure agreement to participate. These documents are physically maintained in WSIC. All agencies providing criminal intelligence to WIN are operating under Agency User Agreements and Individual User Agreements, which are physically maintained by WSIC.

All members of WSIC are required to review and adhere to the Privacy Policy. WSIC will provide a printed copy of this policy upon request to all entities participating in WSIC and will require a written acknowledgement to comply with this policy and the provisions it contains. The Privacy Policy will also be posted on a public-facing website for review.

WSIC has adopted internal operating policies and/or procedures that are in compliance with applicable laws and regulations protecting privacy, civil rights, and civil liberties including but not limited to, the U.S. Constitution, the Wisconsin Constitution, and the Wisconsin Statutes, including Wis. Stat. §§ 19.31-19.37 (Wisconsin public records law); Wis. Stat. § 19.62-19.80 (personal information practices); Wis. Stat. § 100.525 (Telephone records; obtaining, selling, or receiving without consent); Wis. Stat. § 134.98 (Notice of unauthorized acquisition of personal information); Wis. Stat. § 943.201 (Unauthorized use of an individual's identifying information); Wis. Stat. § 943.203 (Unauthorized use of a business's identifying information); Wis. Stat. § 995.50 (Right of privacy).

E. Membership of WSIC

Members of WSIC include personnel assigned to WSIC by the Wisconsin Department of Justice-Division of Criminal Investigations, as well as other state, federal, and local agencies operating under a memorandum of understanding (MOU) with WSIC outlining and agreeing to the terms for such participation.

Members assigned to WSIC will be expected to participate in a capacity as deemed appropriate by the member's agency and will have the ability to be virtually connected to WSIC. Agencies utilizing WIN are considered contributors or source agencies for WSIC.

F. Governance and Oversight

Primary responsibility for the operation of WSIC is assigned to the Special Agent in Charge (SAC) (Fusion Center Director) of WSIC, who is under the direct command of the Special Operations Bureau Director in the Division of Criminal Investigation (DCI) who in turn reports to the DCI Administrator. WSIC SAC (or their designee) will have the responsibility for coordinating personnel from WSIC and other agencies. Each person assigned to WSIC, users of WIN or participants utilizing WSIC resources are personally responsible and will be personally accountable for adhering to this policy, maintaining information standards, processes, procedures and practices.

The Department of Justice Administrator of Legal Services and the Division of Criminal Investigation Administrator will designate a well qualified individual to serve as the Privacy Officer (PO) for WSIC. Responsibilities will include: Oversight of information privacy issues, implementation of Privacy Policy requirements related to the ISE, periodic privacy policy review and update, and handling reports and complaints regarding alleged errors and Privacy Policy violations. The PO shall be trained and will receive assistance from the Division of Legal Services of the Wisconsin Department of Justice.

G. Definitions

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

H. Information

1. WSIC may gather, receive, analyze, disseminate and retain information that is useful in crime analysis or situational assessment reports for the administration of justice and public safety when that information is:

    - based upon reasonable suspicion that the information relates to a credible criminal predicate or a potential threat to public or law enforcement safety; or
    - based upon reasonable suspicion that an identifiable individual or organization has committed, is committing, or is planning to commit criminal conduct or activity that presents a threat to any individual, the community or the nation; or
    - relevant to an active or ongoing investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders or sentences by response of any such incident or response; or the prevention of crime reasonably believed likely to occur without such preventative effort.

    This information must be such that the source of the information is reasonably believed to be reliable and is verifiable or, when appropriate, the limitations on the reliability or veracity of the information are clearly stated; and the information must be collected in a fair and lawful manner, not otherwise prohibited by law, and with the consent of the affected individual to share the information being clearly noted when such consent has been provided.

2. WSIC 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 race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation. Information related to these factors may only be retained if reasonably related to the authorizations in Paragraph H.1 above and necessary to the execution of those authorizations.

3. WSIC will retain information that is based on mere suspicion, such as tips and leads or suspicious activity reports (SARs), only for the purposes and length of time allowed under the limitations established by 28 CFR part 23 where applicable.

4. WSIC requires certain basic descriptive information to be entered and electronically associated with data (or content) or SARs that are to be accessed, used, and disclosed, including:
   - The name of the originating department or source agency;
   - The date the information was collected and to the extent possible, the date its accuracy was last verified;
   - The title and contact information for the person to whom questions regarding the information should be directed and who is accountable for the decision to submit the information and assuring it is believed to otherwise conform to WSIC submission standards;
   - Any particular information privacy or other similar limitations on access, use or disclosure of the information. The nature of the limitation or restriction will be included.

5. WSIC personnel will, upon receipt of information, to include SAR information, assess the information to determine its nature and purpose. WSIC personnel will assign information to categories to indicate the result of the assessment, such as:
   - Whether the information is general data, tips and leads data, suspicious activity reports, or criminal intelligence information;
   - The nature of the source (for example, anonymous tip, interview, public records, private sector);
   - 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 had not as yet been assessed
   - The validity of the content:
     - Confirmed – the information has been corroborated by a trained law enforcement analyst or officer or other reliable source
     - Doubtful – the information is of questionable credibility but cannot be discounted based on the knowledge and skills of the reviewer
     - Cannot be judged – the information cannot be confirmed at the time of review
   - 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 through their own investigation.
   - Due diligence will be exercised by source or submitting agency as well as WSIC personnel in determining source reliability and content validity. WSIC personnel may

reject information as failing to meet any criteria for inclusion, and return such information to the submitting party with an indication of why it was rejected.
- Information determined to be unfounded will be purged from WIN and from the shared space.

6. WSIC personnel upon receipt of designated SAR information will review and vet the SAR information using the most current SAR vetting tool from the Nationwide SAR Initiative Program Management Office to determine whether the information qualifies as an ISE-SAR for contribution to the shared space.

7. At the time a decision is made to retain information in WSIC databases, including contributing ISE-SAR information to the shared space, WSIC personnel will manage the information in order to:
   - Protect an individual's right of privacy and civil rights and civil liberties;
   - Protect confidential sources and police undercover techniques and methods;
   - Not interfere with or compromise pending criminal investigations; and
   - Provide any legally required protection based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

8. The retention or classification of existing information will be reevaluated whenever:
   - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
   - New information is gathered that has an impact on confidence (source reliability and content validity) in the information.
   - There is a change in the use of the information affecting access or disclosure limitations.
   - Information has been developed that suggests the existing information is no longer of intelligence or investigative value or otherwise no longer warrants retention.

9. WSIC personnel are required to adhere to the following practices and procedures for the storage, access, dissemination, retention, and security of tips and leads and suspicious activity reports (SARs) information.
   - Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
   - Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination).
   - 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 tips, leads, and SAR information to other entities or individuals, including the public, when credible information indicates potential imminent danger to life or property.
   - Retain information long enough to work a tip or lead to determine its credibility and value, assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, meets reasonable suspicion/risen to criminal intelligence) so that an authorized user knows that status and purpose for the retention and will retain the information based upon the retention period associated with the disposition label.
   - Adhere to and follow the center's physical, administrative and technical security measures that are in place for the protection and security of tips and leads information.

I. Acquiring and Receiving Information

1. WSIC will keep a record of the source of all information retained by the center.

2. Information gathering and investigative techniques used by WSIC and affiliated agencies will comply and adhere to the following regulations and guidelines:
   - The center will follow 28 CFR Part 23 with regard to criminal intelligence information.
   - The center will adhere to criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
   - The center will adhere to the obligations of law, including Wisconsin Statutes, as well as any regulations that apply to multi-jurisdictional intelligence databases.

3. Regardless of the criminal activity involved, no information which a user has reason to believe may have been obtained in violation of law shall be entered into the WIN System or submitted to or received by WSIC. If WSIC is notified or otherwise learns that information has been obtained illegally, it will be removed.

4. Agencies that participate in WSIC and provide information to the center are governed by state and local laws and rules governing them, as well as by applicable federal laws. WSIC will contract only with commercial database entities that provide an assurance that they gather personally identifiable information in compliance with local, state, tribal, territorial, and federal laws and that such gathering is not based on misleading information collection practices.

5. WSIC will not directly or indirectly receive, seek, accept, or retain information from:
   - An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if the center knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information; or
   - The source used prohibited means to gather the information.

6. Law enforcement officers and personnel at source agencies and WSIC who acquire SAR information that may be shared with WSIC will be trained to recognize behavior that is indicative of criminal activity related to terrorism. The responsibility for this training resides with the contributing agency.

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

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

J. Information Quality Assurance

1. To the maximum extent practical, WSIC will implement the "Fair Information Practices" as detailed by the Department of Justice's Global Initiative, recognizing that some of the practices (such as allowing individuals about whom information is retained to review the information for accuracy) do not apply to an intelligence-gathering initiative. All contributors of information to WSIC should be familiar with the Global "Fair Information Practices" and will apply those practices to the best extent practicable to the information gathered, retained and reported to WSIC.

2. WSIC will make every reasonable effort to ensure that information sought or retained, to include ISE-SAR information, is derived from dependable and trustworthy sources of information.

3. State, local and Tribal (SLT) agencies, including agencies participating in the Information Sharing Environment (ISE), are primarily responsible for the quality and accuracy of the data accessed by or shared with the center, to include SAR data. At the time of posting to the shared space, ISE-SAR information will be labeled according to the level of confidence in the information to the maximum extent feasible. 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. Originating agencies providing data remain the owners of the data contributed.

4. Information provided through WIN, the shared space or by WSIC is not designed to provide users with information upon which official actions may be taken. The mere existence of records in WIN or the shared space or provided by WSIC should not be used to provide or establish probable cause for an arrest, be documented in an affidavit for a search warrant or serve as documentation in court proceedings. Only the facts, which led to the entry of the record into the WIN or the shared space, can be used to establish probable cause in an affidavit. The source agency should be contacted to obtain and verify the facts needed for any official action.

5. WSIC will investigate, in a timely manner, alleged errors and deficiencies, to encompass ISE-SAR information, and will correct, delete or refrain from using protected information found to be erroneous or deficient. WSIC will advise the appropriate data owner in writing (to include electronic notification) if its data contributed to the center is found to be inaccurate, incomplete, out of date, or unverifiable. In addition, WSIC will provide documented electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by WSIC because it is erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of an individual data subject may be affected. Any needed corrections to or deletions made to ISE-SAR information will be made to such information in the shared space.

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

K. Collation and Analysis

1. Information acquired by WSIC, to include ISE-SAR information, or accessed from other sources will only be analyzed by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved and trained accordingly.

2. Information acquired by WSIC, to include ISE-SAR information, or accessed from other sources is analyzed according to priorities and needs and will only be analyzed to:
   - Provide crime analysis or situational assessment reports for the administration of justice and public safety.
   - Further crime/terrorism prevention, enforcement, force deployment, or prosecution objectives and priorities established by WSIC, 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 activities, including criminal solicitations, criminal conspiracies, and/or attempts to obstruct justice.

L. Merging Records

1. 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.

2. Sufficient identifying information 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. The reality that identities can be stolen by those who perpetrate crimes makes the verification of factors in support of merging of records particularly important. Innocent individuals' identities may be utilized by criminals and merging of an innocent individual's information into records related to the criminal without explanation or other appropriate safeguards against misinterpretation of the information should not occur.

3. 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 and a reminder that identity theft may be the reason there has been the partial match.

M. Sharing and Disclosure

1. Credentialed security access will be utilized to control:
   - What information a class of users can have access to;
   - What privacy fields in ISE-SAR shared space a class of users have access to;
   - What information a class of users can add, change, delete, or print; and
   - To whom the information can be disclosed and under what circumstances.

2. Personal identifiable information (such as social security numbers) will be removed from disseminated products as appropriate, specifically when dissemination includes non-law enforcement entities.

3. WSIC will operate according to the Third Agency Rule unless otherwise instructed by law, rule or Memorandum of Understanding, therefore, WSIC participating agencies may not unilaterally disseminate information received from WSIC without approval from the originator of the information. There is a presumption that all records contributed to WIN and the shared space are intended to be shared with other agencies participating in said systems.

4. Records retained by WSIC may be accessed or disseminated *to those responsible for law enforcement, public health and safety protection, prosecutions, or justice purposes derived from criminal investigations or prosecutions* only for such purposes and then only in the performance of official duties in accordance with applicable laws, regulations, and procedures. An audit trail will be kept of access by or dissemination of WIN information to such persons. Information gathered and records retained by WSIC may be accessed or disseminated *for specific purposes* upon request by persons authorized by law to have such access and only for those users or purposes specified by law.

5. As long as information constitutes active criminal investigative or active criminal intelligence information, or is otherwise within the scope of an applicable exemption or confidentiality provision of Wisconsin law, information gathered and records retained by WSIC, to include ISE-SAR information and those records within WIN and the shared space, will not be released to the public. ISE-SAR information posted to the shared space by WSIC may be disclosed to a member of the public only if the information is defined by law to be public record or otherwise appropriate for release to further WSIC mission and is not exempt from disclosure by law.

6. WSIC shall not confirm the existence or nonexistence of information, to include WIN records or ISE-SAR information to any person or agency that would not be eligible to receive the information itself. ISE-SAR information will not be provided to the public if, pursuant to applicable law it is:
   - Required to be kept confidential or exempt from disclosure.
   - Classified as investigatory records and exempt from disclosure.
   - Protected federal, state, or tribal records originated and controlled by the source agency that cannot be shared without permission.
   - A violation of an authorized nondisclosure agreement.

7. Information that is no longer active criminal investigative or active criminal intelligence information will be promptly purged in a manner consistent with Wisconsin law and 28 CFR part 23.

8. Information gathered and records retained by WSIC will not be sold, published, exchanged, or disclosed for commercial purposes. It will not be disclosed or published without prior notice to the contributing agency. Information will not be disseminated to unauthorized persons.

N. Redress

1. Information that is retained by WSIC, to include WIN records and ISE-SAR information, is considered active intelligence or criminal investigative information and, therefore, is exempt from public disclosure. If an individual wants to review information that has been documented in an intelligence file or system or as part of an investigative case management system, a formal public records request must be made via the Wisconsin Department of Justice. WSIC and all participating agencies will refer complaints and redress issues to the Wisconsin Department of Justice. A copy of any referrals will be keep by the referring agency.

2. The existence, content, and source of the information will not be made available to an individual (when there is legal basis for denial). To the extent allowed by law, information will not be verified or released if:
   - The disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution; or
   - The disclosure would endanger the health or safety of an individual, organization, or community; or
   - The disclosure would compromise law enforcement or criminal intelligence strategies, methods, or tactics; or
   - The information's use and dissemination is limited by federal, state, or local law; or
   - The information is classified, sensitive, confidential, or otherwise of a restricted use or nature; or
   - The information is in a criminal intelligence system.

3. If a public records request was made through the Wisconsin Department of Justice and the decision is made to release information, any complaints or objections to the accuracy or completeness of information retained about him or her should be made in writing and handled through the Department of Justice. The individual would be required to provide a written request to modify the documentation, remove the record and provide adequate reasoning for the request. The information would then be submitted to the Wisconsin Department of Justice for consideration.

4. The individual to whom information has been disclosed will be provided with a justification and the procedures for appeal, if the request for correction is denied by WSIC or the originating agency. Upon denial, the individual will be informed of the procedures for correcting or modifying the information. All appeals with be handled by the Wisconsin Department of Justice. The Department of Justice will keep a record of all requests and of what information is disclosed to an individual.

5. If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information ***resulting in specific, demonstrable harm to said individual***, and that such information about him or her is alleged to be held by WSIC, regardless of source or originating agency, WSIC must inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for

corrections and the resulting action, if any. Complaints must be directed to the Administrator of Legal Services at the following address: Wisconsin Department of Justice, 17 W Main Street, Madison, WI, 53703.

6. The Department of Justice will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of any ISE-SAR that contains information in privacy fields that identifies the individual. However, any personal information will be reviewed and corrected in or deleted from the ISE-SAR shared space within 30 days if the information is determined to be erroneous, includes incorrectly merged information, or is out of date.

O. Security Safeguards

1. WSIC will operate in a secure facility protecting the facility from external intrusion. WSIC will utilize secure internal and external safeguards against network intrusions, to include ISE-SAR information and WIN records. Access to WSIC databases, to include WIN and the ISE-SAR shared space, from outside the facility will only be allowed over secure networks.

2. WSIC will store information, to include WIN records and ISE-SAR information, in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

3. Access to WSIC information, to include WIN records and ISE-SAR information, will only be granted to WSIC members whose position and job duties require such access and who have successfully completed a background check and appropriate security clearance, if applicable, and has been selected, approved, and trained accordingly.

4. Queries made to WSIC data applications, to include WIN and the ISE-SAR shared space, will be logged into the data system identifying the user initiating the query. WSIC will utilize watch logs to maintain audit trails of requested and disseminated WIN and ISE-SAR information. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

5. WSIC will, in the event of a data security breach, consider notifying an individual about whom personal information was or is reasonably believed to have been compromised or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. Any notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the breach or any measure necessary to determine the scope of the breach and, if necessary, to restore the integrity of the system.

P. Information Retention and Destruction

1. All WIN information will be reviewed for record retention (validation or purge) every five (5) years, as stated by 28 CFR Part 23. When information has no further value, it will be purged, destroyed, and deleted or returned to the contributing agency. Notification of proposed destruction of records will be provided to the contributor during the review period. For purposes of meeting the Wisconsin Department of Justice's records retention rules and guidelines, all information contained in WIN is considered a "copy" of the information, with the original being in the care and control of the contributor. Destruction of information within WIN is destruction of copies, and may be under different guidelines and restrictions than those applicable to the original record in the custody of the contributor. Each contributor is

solely responsible for its compliance with Wisconsin Statutes and its related records retention and destruction obligations.

2. A record of information to be reviewed for retention will be generated by WSIC using the WIN system. Notice will be given to the individual who submitted the information at least 30 days prior to the required review and validation/purge date. Agreement to destroy or return information or records will be presumed if the applicable information is not validated within the specified time period.

3. WSIC will retain ISE-SAR information in the shared space to permit the information to be validated or refuted, its credibility and value to be reassessed, and to the degree possible a "disposition" label will be assigned so that subsequent authorized users know the status and purpose for the retention.

Q. Accountability and Enforcement

Q1. Information System Transparency

1. WSIC will be open with the public in regard to information and intelligence collection practices. WSIC's privacy policy will be provided to the public for review via the WiWATCH website.

2. WSIC, through its Privacy Officer when appropriate, in consultation with the Wisconsin Department of Justice will be responsible for receiving and coordinating a response to inquiries and complaints about privacy, civil rights, and civil liberties protections related to ISE-SAR information, WIN and the operations of the Wisconsin Statewide Information Center.

Q2. Accountability

1. WSIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law.

2. WSIC will follow procedures to evaluate the compliance of authorized users of WIN. Records of audits will be maintained by WSIC. Any audits conducted will be in such a manner as to protect the confidentiality, sensitivity, and privacy of the ISE-SAR information and WIN records as well as any related documentation.

3. The members of WSIC or other authorized users of WIN may report violations or suspected violations of Privacy Policy to WSIC SAC, the Privacy Officer or their designee.

4. If an authorized user is found to have violated the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, WSIC may**,** in consultation with the Wisconsin Department of Justice:
   - Suspend or discontinue access to information by the user;
   - Suspend, demote, transfer, or terminate the person, as permitted by applicable personnel policies;
   - Apply administrative actions or sanctions as provided by applicable personnel rules and regulations or as provided in agency personnel policies;

- If the user is from an agency external to the center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

5. WSIC's Governance Board in consultation with WSIC SAC and Division of Criminal Investigation, will annually review and update as appropriate, the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.

Q3. Enforcement

WSIC reserves the right to restrict the qualifications and number of personnel having access to WSIC information, to include WIN records, and to suspend or withhold service to any personnel violating the privacy policy. WSIC reserves the right to deny access to WIN or WSIC products to any participating agency or individual user who fails to comply with the applicable restrictions and limitations of WSIC privacy policy.

R. Training

All WSIC staff submitting, receiving or disseminating criminal intelligence or criminal investigative information or suspicious activity reports or having access to the shared space and ISE-SAR information will participate in annual training programs. Training subjects will include implementation of and adherence to privacy, civil rights and civil liberties policies and protections pertinent to the scope of their employment and access to said information. WSIC's primary training program will be delivered by the WSIC Privacy Officer. An alternative training program is delivered on-line through the U.S. Department of Justice, Bureau of Justice Assistance's Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Online Training Program at https://www.ncirc.gov/28cfr/Default.aspx.

Appendix A
Terms and Definitions

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

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

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

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

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

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

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

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

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

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

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

Center – Center refers to the Wisconsin Statewide Information Center or WSIC

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

Civil Rights—The term "civil rights" is used to imply that the state (or government) has a role in ensuring all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

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

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

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

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

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

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

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

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

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

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

WSIC Governance Board- Comprised of representatives from the following agencies:

The Wisconsin Adjutant General
(Governor's Homeland Security Advisor)
Wisconsin Chiefs of Police Association
Wisconsin Fire Chiefs Association
Badger Sheriff's Association
Federal Bureau of Investigation
Department of Health Services
Department of Agriculture
Wisconsin Emergency Management
Transportation Security Administration
Wisconsin State Patrol
Wisconsin Tribal Police Chiefs Association
Southeastern Wisconsin Threat Analysis Center (STAC)
Department of Natural Resources
United States Attorney's Office
Wisconsin Department of Justice
Wisconsin Department of Corrections
U.S. Marshals Service, Western District of Wisconsin
Wisconsin Capitol Police
U.S. Department of Homeland Security

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transporter Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system. They are designed to:

1. Define agency purposes for information to help ensure agency uses of information are appropriate. ("Purpose Specification Principle")

2. Limit the collection of personal information to that required for the purposes intended. ("Collection Limitation Principle")

3. Ensure data accuracy. ("Data Quality Principle")

4. Ensure appropriate limits on agency use of personal information. ("Use Limitation Principle")

5. Maintain effective security over personal information. ("Security Safeguards Principle")

6. Promote a general policy of openness about agency practices and policies regarding personal information. ("Openness Principle")

7. Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency. ("Individual Participation Principle")

8. Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. ("Accountability Principle")

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

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

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

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

Homeland Security Information—As defined in Section 482(f)(1) of the Homeland Security Act, homeland security information means any information possessed by a federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual response to a terrorist act.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a compound of such data as a

given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

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

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

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

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

Persons—Executive Order 12333 defines "United States persons" as a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

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

Privacy Fields—Data fields in ISE-SAR IEPDs that contain personal information.

Privacy Policy—A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and

access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing. The process should maximize the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

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

Public does not include:

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

Public Access—Public access relates to what information can be seen by the public, that is, information whose availability is not subject to privacy interests or rights.

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

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

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

Retention—Refer to "Storage."

Right to Privacy—The possible right to be left alone, in the absence of some reasonable public interest in a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating that right.

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

Security—Security refers to the range of administrative, technical, and physical mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Shared Space—A networked data and information repository which is under the control of WSIC and takes in information and intelligence from submitting agencies which provide terrorism-related information, applications, and services to other ISE participants.

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

SLT—State, Local and Tribal

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

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

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

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

Source Agency—The agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

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

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

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

Terrorism Information—Consistent with Section 1016(a)(4) of IRTPA, all information relating to the (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism, (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations, (C) communications of or by such groups or individuals, of (D) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism Related Information—In accordance with IRTPA, as recently as amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)1) (6 U.S.C. § 482(f)1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

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

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

Tips and Leads Information or Data—Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity

reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data.

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

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

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

WSIC Personnel – Full or part-time employees assigned to be physically located at WSIC by their agencies.