Wyoming Information Analysis Team

1 May 2017

Privacy, Civil Rights, and Civil Liberties Policy

Revision 1.1, dated 26 June.

Table of Contents

Mission and Purpose Statement

Mission Statement - The mission of the Wyoming Information Analysis Team (WIAT) is to collect, store, analyze and disseminate information and intelligence data on crimes, both real and suspected, to the law enforcement community, government officials and private industry concerning dangerous drugs, fraud, organized crime, terrorism and other criminal activity for the purposes of decision making, public safety and proactive law enforcement while ensuring the rights and privacy of citizens. This is done while following appropriate privacy and civil liberties safeguards as outlined in the principles of the U.S. Privacy Act of 1974 (as amended) Fair Information Practice Principles to ensure that the information privacy and other legal rights of individuals and organizations are protected (see definitions of "Fair Information Principles" and "Protected Information" in Appendix A, Definitions.)

Purpose Statement: The purpose of this privacy, civil rights, and civil liberties protection policy (Privacy Policy) is to promote WIAT end-user conduct that complies with applicable federal and state law; to assist the center and its users in properly handling Personally Identifiable Information (PII) or Sensitive PII; and to protect individual privacy, civil rights, civil liberties, and other protected interests of the individuals whose data the WIAT collects, uses, stores, and disseminates.

Policy Applicability and Legal Compliance

1) All WIAT personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, and other authorized users will comply with the center's privacy policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment (ISE) participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

2) The WIAT will provide a printed or electronic copy of this policy to all center and non-center personnel who provide services and to participating agencies and individual users and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

3) All WIAT personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. Constitution, Wyoming State Constitution, Wyoming statutes, the Intelligence Reform

and Terrorism Prevention Act (IRTPA), and 28 Code of Federal Regulations (CFR) Part 23, 6 CFR Part 29.[1, 2]

4) The WIAT has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to those listed above.

Governance and Oversight

1) The Wyoming Division of Criminal Investigation (DCI) has the primary responsibility for the operation of the WIAT, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Team Leader/Director of the center.

2) The WIAT is guided by a designated privacy oversight team that ensures privacy and civil rights are protected in accordance with this Privacy Policy and by the center's information-gathering and collection, retention, and dissemination processes and procedures. The team will annually review and update the policy in response to any changes in law and implementation experience, including the results of audits and inspections.

3) The WIAT's privacy team is guided by a trained Privacy Officer who is appointed by the Team Leader/Director of the center. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the Center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at the following address: dci.intel@wyo.gov.

4) The WIAT's Privacy Officer ensures that enforcement procedures and sanctions outlined in "Accountability and Enforcement" are adequate and enforced.

Definitions

Please refer to Appendix A: Terms and Definitions for a full list of terms used throughout this Privacy Policy.

[1] Specific Wyoming statutes: Wyoming State Constitution Article 1, Sections; § 2, § 3, § 4, § 6, § 17, § 18, § 20, Wyoming Statutes: § 9-1-627 and § 16-4-201 to 16-4-204.

[2] Please refer to Appendix B for a listing of federal laws relevant to seeking, retaining, and disseminating justice information.

Information

1) WIAT will seek or retain information that:
    a. Is based upon reasonable suspicion that the information constitutes a credible criminal predicate or a potential threat to public safety; or
    b. Is 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
    c. Is 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; or
    d. Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
    e. Is 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 is clearly stated; and
    f. The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

    The WIAT may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.

2) The WIAT will not seek or retain information, and information-originating agencies will agree not to submit 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, gender identity, or sexual orientation. Information related to these factors may be retained if there is a reasonable relationship or relevance to such information and the effort to detect, anticipate, or prevent criminal activity and this information is not the sole basis for retention or indexing. When there is a reasonable basis to believe a criminal relationship exists, the information concerning the criminal conduct or activity may be retained or indexed in accordance with the provisions of this policy (see Information Retention and Destruction); however, it is the responsibility of the source agency or WIAT personnel to ascertain and clearly affirm the relationship to the key element of criminal activity prior to the retention or indexing of the information.

3) The WIAT applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:
    a. The information is protected information (as defined by the center to include personal information – refer to "protected information" and "personal information" in Appendix A of this policy) and, to the extent expressly provided in this policy, includes organizational entities.

b. The information is subject to state and federal laws restricting access, use, or disclosure.

4) WIAT personnel will, upon receipt of information, assess the information to determine its nature, usability, and quality. Members of WIAT will assign information to categories (or ensure that the originating agency has assigned categories to the information) to indicate the result of the assessment, such as:
    a. Whether the information is tips/leads data, suspicious activity reports, criminal history, intelligence information, or case records.
    b. The nature of the source as it affects veracity (for example, anonymous tip, interview, public records, private sector);
    c. The reliability of the source:
        i. Reliable – the source has been determined to be reliable
        ii. Possibly Reliable – the information given by the source has typically been reliable
        iii. Unreliable – the reliability of the source is doubtful or has been determined to be unreliable
        iv. Unknown – the reliability of the source cannot be judged or has not as yet been assessed
    d. The validity of the content:
        i. Confirmed – the information has been corroborated by a trained law enforcement analyst or officer or other reliable source
        ii. Possibly True – the information has not been corroborated by a trained law enforcement analyst or officer or other reliable source but is consistent with past accounts and possibly true
        iii. Improbable– the information is of questionable credibility but cannot be discounted based on the knowledge and skills of the reviewer
        iv. Unknown – the information cannot be confirmed at the time of review
    e. Unless otherwise indicated by the source or submitting agency, source reliability is deemed to be "unknown" and content validity "unknown." In such case, users must independently confirm source reliability and content validity with the source or submitting agency or through their own investigation.
    f. A record of the source of all information sought and collected will be kept.
    g. Due diligence will be exercised by source or submitting agency as well as WIAT personnel in determining source reliability and content validity. WIAT 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.
    h. Intelligence determined to be unfounded will be purged from the intelligence database.

5) At the time a decision is made by the WIAT to retain information, it will be labeled (by record or data set), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:
    a. Protect confidential sources and police undercover techniques and methods.
    b. Not interfere with or compromise pending criminal investigations.
    c. Protect an individual's right of privacy or his or her civil rights and civil liberties.

d. Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6) The labels assigned to existing information under (the Information section) of this Privacy Policy will be reevaluated whenever:
    a. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
    b. There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7) WIAT personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of suspicious activity report (SAR) information. Center personnel will:
    a. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.
    b. Store the information, which may be based on only being "reasonably indicative," using the same storage method used for data which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
    c. Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).
    d. Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
    e. Retain information for up to one business day in order to investigate unvalidated SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that subsequently authorized users know the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label (for additional information on the WIAT's retention schedules, refer to Information Retention and Destruction, below).
    f. Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of SAR information. SAR

information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

8) The WIAT incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as the information privacy, civil rights, and civil liberties.

9) The WIAT will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10) WIAT requires certain basic descriptive information to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding the access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information may include:
    a. The name of the originating department, or source agency;
    b. The name of the center's justice information system from which the information is disseminated.
    c. The date the information was collected and to the extent possible, the date its accuracy was last verified;
    d. 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 WIAT submission standards;

11) The WIAT will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on sensitivity or classification.

12) The WIAT will keep a record of the source of all information sought and collected by the center.

Acquiring and Receiving Information

1) Information gathering and access and investigative techniques used by WIAT and affiliated agencies will comply with and adhere to the following regulations and guidelines:
    a. 28 CFR Part 23 with regard to criminal intelligence information.
    b. The Federal Privacy Act Fair Information Practice Principles (under certain circumstances, there may be exceptions to the Fair Information Practice

Principles, based, for example, on authorities paralleling those provided in the Federal Privacy Act; state, local, or tribal law; or center policy.)

c. Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP).
d. Constitutional Provisions; Wyoming Statute § 9-1-627; and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

2) The WIAT's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3) The WIAT's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals and/or organizations involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4) Information-gathering and investigative techniques used by the WIAT will be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain. To the extent feasible, information will be gathered first from publicly available sources. If information is not available publicly, it may be collected (in progressive order) from cooperating or consenting sources, lawful intelligence techniques, or other legal means such as a warrant.

5) External agencies that access the WIAT’s information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

6) The WIAT does not independently contract with commercial database entities. The Wyoming Attorney General's Office and Wyoming DCI oversee contracting in accordance with state, and federal regulations.

7) The WIAT will not directly or indirectly receive, seek, accept, or retain information from:
    a. An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
    b. An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

8) 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 information

or intelligence databases or submitted to or received by WIAT. If WIAT is notified or otherwise learns the information has been obtained illegally, the information will be removed.

Information Quality and Assurance

1) WIAT will make every reasonable effort to ensure the information sought or retained is derived from dependable and trustworthy sources of information, and is accurate, current and complete. This includes the relevant context in which it was sought or received and other related information. The collected information will be merged with other information about the same individual or organization only when the applicable standard (refer to "Merging Records") has been met.

2) The WIAT investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

3) The labeling of retained information will be reevaluated by the WIAT or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

4) The WIAT will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

5) Originating agencies external to the WIAT are responsible for reviewing the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

6) The WIAT will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

Collation and Analysis

1) Information acquired or received by WIAT or accessed from other sources will be analyzed only by qualified individuals, who have successfully completed a background

check, appropriate security clearance, and if applicable, and have been selected, approved and trained accordingly.

2) Information subject to collation and analysis is information as defined and identified in the Information Section of this Privacy Policy.

3) Information acquired or received by WIAT or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:
    a. Further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by WIAT.
    b. 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 terrorism).

Merging Records

1) The set of identifying information sufficient to allow merging by the WIAT will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; or driver's license number. 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.

2) If the matching requirements cannot fully be met but there is an identified partial match (for example, the name and only a partial match of the date of birth), the information may be associated by the WIAT only if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

Sharing and Disclosure

1) Credentialed, role-based, access criteria will be used by the WIAT, as appropriate, to control:
    a. What information a class of users can have access to;
    b. What information a class of users can add, change, delete, or print; and
    c. To whom the information can be disclosed and under what circumstances.

2) The WIAT adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

3) Access to or disclosure of records retained by WIAT will be provided only to persons within the WIAT or in other governmental agencies who are authorized to have access. Said access and disclosure will only be for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes. In addition, access or disclosure will be provided only for the performance of official duties in accordance with Wyoming Statute § 9-1-627 and other laws and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the center.

4) Agencies external to WIAT may not disseminate information accessed or disseminated from the WIAT without approval from the WIAT or other originator of the information.

5) Records retained by the WIAT may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

6) The WIAT will make every attempt to safeguard Personally Identifiable Information (PII) from loss, compromise, or unauthorized disclosure. Social Security Numbers, criminal records, financial account information, and account passwords are considered to be Sensitive PII and will only be shared in a manner compliant with applicable state and federal laws governing these types of information. In addition, whenever feasible, WIAT personnel should encrypt Sensitive PII prior to mailing or electronically transmitting it to an outside agency.

7) Information gathered or collected and records retained by the WIAT may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept indefinitely by the center.

8) Information gathered or collected and records retained by WIAT may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or is otherwise appropriate for release to further the Team's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the Team for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

9) Information gathered or collected and records retained by WIAT will not be:
    a. Sold, published, exchanged, or disclosed for commercial purposes.

b. Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
c. Disseminated to persons not authorized to access or use the information.

10) All intelligence and records, collected and stored within the intelligence system are prohibited from being released to the public or any agency not outlined by Wyoming State Statute § 9-1-627. This includes the release of information confirming the existence or nonexistence of information on file at WIAT.

11) Should a request for information disclosure be received from an individual not authorized access according to Wyoming Statute § 9-1-627, the request will be referred to the WIAT Team Leader or designee. The WIAT Team Leader or designee will document the name, date of request, and concern of the requester and forward the request to the appropriate assistant attorney general.

12) There are several categories of records that will ordinarily not be provided to the public:
    a. Records required to be kept confidential by law are exempted from disclosure requirements under Wyoming Statutes § 16-4-201 to 16-4-203.
    b. Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606 and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
    c. Investigatory records of law enforcement agencies that are exempted from disclosure requirements under Wyoming Statutes § 16-4-201 to 16-4-203. However, certain law enforcement records must be made available for inspection and copying under Wyoming Statutes § 16-4-201 to 16-4-203.
    d. A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under Wyoming Statutes § 16-4-201 to 16-4-203. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
    e. Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under Wyoming Statutes § 16-4-201 to 16-4-203, be shared without permission.
    f. A violation of an authorized nondisclosure agreement under Statutes § 16-4-201 to 16-4-203.

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

14) Information retained by WIAT that is considered active intelligence or open/ongoing criminal investigative information is exempt from public disclosure in accordance with Wyoming Statute § 9-1-627.

15) Public records requests for information held by the WIAT may be submitted through the Wyoming Attorney General's Office, who determines whether information may be released. If the decision is made to release information, the request will be submitted to the WIAT for action. The center's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

Redress

1) Redress will be limited to information that is subject to disclosure under Wyoming Statute § 16-4-203. The existence, content, and source of the information will not be made available by WIAT to an individual when:
    a. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution. Wyo. Stat. § 16-4-203(b)(i)
    b. Disclosure would endanger the health or safety of an individual, organization, or community. Wyo. Stat. § 16-4-203(b)(vi)
    c. The information is in a criminal intelligence information system subject to 28 CFR Part 23 (see 28 CFR § 23.20(e)). Wyo. Stat. § 16-4-203(b)(i)
    d. The information relates to Wyo. Stat. § 16-4-203(a)(ii)
    e. The information source does not reside with the center. Wyo. Stat. § 16-4-203(a)(ii)
    f. The WIAT did not originate and does not have a right to disclose the information.

2) If the information does not originate with the agency, the requestor will be referred to the originating agency, if appropriate or required, or the agency will notify the source agency of the request and its determination that disclosure by the agency or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

Corrections

1) If a public records request is submitted through the Wyoming Attorney General's Office and the decision was made to release information, any complaints or objections to the accuracy or completeness of information retained about the person should be made in writing and handled by the Wyoming Division of Criminal Investigation. The individual will be required to provide a written request to modify the documentation, remove the record and provide adequate reasoning for the request. The information will then be submitted to WIAT for consideration. A record will be kept of all requests for corrections and the resulting action, if any.

Appeals

1) The individual who has requested disclosure or to whom information has been disclosed will be provided with a justification. If the request for correction is denied by WIAT or the originating agency, the individual will be informed of the procedures for disputing the decision. All appeals will be handled by the Wyoming Attorney General's Office, Division of Criminal Investigation. A record will be kept of all requests and of what information is disclosed to an individual.

Complaints

1) If an individual has a complaint or objection to the accuracy or completeness of terrorism-related protected information held by WIAT, the individual will be informed by WIAT of the procedure for submitting (if needed) and resolving such complaints. Said information must be exempt from disclosure, have been or may be subject to being shared through the ISE, and allegedly have resulted in demonstrable harm to the complainant. Complaints will be received by the WIAT's Team Leader or designee. The Team Leader and/or designee will acknowledge the complaint and notify the complainant the matter will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law.
    a. Individuals handling complaints can be contacted at dci.intel@wyo.gov, or 307-777-7181.

2) If the information did not originate with WIAT, the Team Leader or designee will notify the originating agency in writing or electronically within ten (10) days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. The information held by WIAT pertaining to the subject of a complaint will be reviewed within thirty (30) days and confirmed or corrected/purged if determined to be inaccurate or incomplete, including incorrectly merged information, or information that is out of date. If there is no resolution within thirty (30) days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint, whether by WIAT or the originating agency.

3) To delineate protected information shared through the ISE from other data, the WIAT maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

Security Safeguards

1) The WIAT Team Leader and/or designee is designated and trained to serve as the security officer.

2) The WIAT will operate in a secure facility protected from external intrusion. The Center will utilize secure internal and external safeguards against network intrusions. Access to the Center's databases from outside the facility will be allowed only over secure networks.

a. All authorized visitors will be escorted by designated authorized personnel for the duration of their visit.

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

4) The WIAT will store information in a manner such that it cannot be added to, modified, accessed, or destroyed, or purged except by personnel authorized to take such actions.

5) Access to WIAT information will be granted only to Center personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

6) Queries made to the WIAT's data applications will be logged into the data system identifying the user initiating the query.

7) The WIAT will maintain audit trails of requested and disseminated information.

8) To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

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

Information Retention and Destruction

1) All applicable information will be reviewed for record retention (validation or purge) by the WIAT at least every five (5) years, as provided by 28 CFR Part 23.

2) When information has no further value or meets the criteria for removal according to the WIAT's retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.

3) The WIAT will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

4) No approval will be required from the originating agency before information held by the WIAT is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

5) Notification of proposed destruction or return of records may or may not be provided to the originating agency by the WIAT, depending on the relevance of the information and any agreement with the originating agency.

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

Accountability and Enforcement

1) The WIAT will be open with the public with regard to the center's information policies and procedures by providing the privacy policy on the DCI web page at http://wyomingdci.wyo.gov.

2) The WIAT's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Officer can be contacted at dci-intel@wyo.gov.

Accountability

1) The audit log of queries made to the WIAT will identify the user initiating the query.

2) The WIAT will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of one year of requests for access to information for specific purposes and of what information is disseminated

3) The WIAT will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least annually and a record of the audits will be maintained by the Privacy Officer of the center.

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

5) The WIAT will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by the center's Privacy Officer or designee. The Privacy Officer or designee has the option of conducting a random audit, without announcement, at any time and without prior notice

to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).

6) The WIAT's privacy team, guided by the appointed Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

Enforcement

1) If center personnel, a participating agency, or an authorized user is found to be in willful noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Team Leader/Director of the WIAT will:
    a. Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
    b. Suspend, demote, transfer, or terminate center personnel, as permitted by applicable personnel policies.
    c. Apply administrative actions or sanctions as provided by DCI rules and regulations or as provided in agency/center personnel policies.
    d. If the authorized user is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
    e. Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2) The WIAT reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the center's privacy policy.

Training

1) WIAT has adopted the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice training (28 CFR Part 23) as the education and training standard for its center personnel who will be accessing intelligence databases, and will also require the following individuals to participate in training programs regarding implementation of and adherence to this privacy, civil rights, and civil liberties policy:
    a. All assigned personnel of the center.
    b. Personnel providing information technology services to the center.
    c. Staff in other public agencies or private contractors providing services to the center.
    d. Users who are not employed by the center or a contractor. (This does not include customers – see Appendix A for definitions of "users" and "customers.")

2) The WIAT will provide training regarding the center’s requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

3) The WIAT's privacy policy training program will cover:
    a. Purposes of the privacy, civil rights, and civil liberties protection policy.
    b. 28 CFR.23 annual training.
    c. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the center.
    d. Originating and participating agency responsibilities and obligations under applicable law and policy.
    e. How to implement the policy in the day-to-day work of the user, whether a paper or systems user.
    f. The impact of improper activities associated with infractions within or through the agency.
    g. Mechanisms for reporting violations of center privacy protection policies and procedures.
    h. The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

4) All WIAT personnel will provide the Team Leader/Director or designee a copy of a training certificate indicating that they have taken all required annual training.

Appendix A: Terms and Definitions

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

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

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

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

Agency—The Wyoming Information Analysis Team (WIAT) and all agencies (state and federal) that access, contribute, and share information in the WIAT justice information system.

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

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

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

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

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

Center—Refers to the WIAT and all agencies that participate in the WIAT.

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

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

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

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

Credentials—Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Customer—An individual or agency who receives information or services from the center, but does not otherwise have direct access to the center's intelligence databases or resources.

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

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

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

Data Incident—The act of violating an explicit or implied security policy. This includes but is not limited to:
-attempts (either failed or successful) to gain unauthorized access to a system or its data;
-unwanted disruption or denial of service;
-the unauthorized use of a system for the processing or storage of data;
-changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

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

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

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

Encryption—Converting data into a form that cannot be easily understood or accessed by unauthorized people.

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) form the backbone of privacy law in the United States and the concepts they include have played a significant role in the development of data protection laws around the globe. Understanding the Fair Information Practice Principles and how they should be implemented is critical to comply with the various privacy laws that protect personal information. These were developed in the early 1970s about mounting concerns about the government use of computerized databases The

FIPPs provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems, although some of the individual principles may not apply in all instances.

The eight FIPPs are:
1. Collection Limitation (Data Minimization): There should be limits to the collection of personal data to that which is both relevant and necessary for the stated purpose of the system and any such data should be obtained by lawful and fair means.
2. Data Quality: Personal data should be collected directly from the individual where practicable, be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. Purpose Specification: The legal authorities and purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
    a) with the consent of the data subject; or
    b) by the authority of law.
5. Security Safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. Openness (Transparency): There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and physical location of the program.
7. Individual Participation: An individual should have the right: a) to obtain from a program, or otherwise, confirmation of whether or not the program has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended
8. Accountability: A program should be accountable for complying with measures which give effect to the principles stated above.

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—Defined in the ISE-SAR Functional Standard, version 1.5.5 as "[a] collaborative effort of two or more Federal, state, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." (Source: Section 511 of the 9/11 Commission Act). State and major urban area fusion centers serve as focal points within the state and local environment for the receipt,

analysis, gathering, and sharing of threat-related information between the Federal government and SLTT and private sector partners.

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

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

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

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

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

Information Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the Information Sharing Environment (ISE) is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of state, local, tribal, and territorial (SLTT) agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—An ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business rules and privacy and civil liberties requirements will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

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

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

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

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

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

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

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

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

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

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets).

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

Need to Know— Need-to-know is the determination by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function

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

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

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

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

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects. See also Personally Identifiable Information.

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

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, 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 United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, ―persons means United States citizens and lawful permanent residents.

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

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

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

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

regulation. For the (federal) intelligence community, protected information includes information about ―United States persons as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.
For state, local, and tribal governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion Center or other state, local, or tribal agency policy or regulation.

Public—Public includes:
- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the Center's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the Center or a participating agency.

Public does not include:
- Employees of the Center or a participating agency.
- People or entities, private or governmental, who assist the Center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the Center is specified in law.

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

Purge—A term that is commonly used to describe methods that permanently erase and remove data from a storage space. There are many different strategies and techniques for data purging, which is often contrasted with data deletion.

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

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

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

Retention— The continued storage of data—in a manner in which the data can be retrieved, used, and re-stored—for compliance or business reasons, consistent with an established policy or protocol.

Right to Know—Based on having legal authority or responsibility, or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, counter-terrorism activity, or other authorized government duty.

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

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

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

Sensitive Personally Identifiable Information—Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples include SSN, financial account number, or account passwords.

Source Agency/Organizations—Thee agency or entity that originates the SAR report (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The source organization will not change throughout the life of the SAR.

Storage—Storage can refer to computer or hard-copy (such as in a filing cabinet) where information can be retrieved by a particular identifier such as a last name**.**

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-Observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity. Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber-attacks, testing of security, etc.

Suspicious Activity Report (SAR)—Official documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state of regional fusion Center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information- Consistent with Section 1016(a)(4) of the 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 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.

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

Tips and Leads Information or Data- Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion. A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than ―reasonable suspicion‖ and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

User—An individual representing a participating agency who is authorized to directly access the center's information and intelligence databases and resources for lawful purposes. This does not include individuals or agencies who receive information or intelligence reporting and support from the center but do not otherwise have direct access to the center's databases and resources.

Appendix B: Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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