

January 2, 2019

**Western Pennsylvania All
Hazards Fusion Center
Privacy Policy**

Table of Contents

Purpose Statement	Page 3
Policy Applicability and Legal Compliance	Page 3
Transparency and Accountability	Page 3
Information	Page 4
Acquiring and Receiving Information	Page 8
Information Quality	Page 9
Collation and Analysis	Page 10
Merging of Information from Different Sources	Page 11
Sharing and Disclosure	Page 11
Redress	Page 13
Information Retention and Destruction	Page 14
Accountability and Enforcement	Page 15
Training	Page 17
Sharing of Information Among Participants	Page 18
Use/Disclosure of Information Originating from Another Participating Agency	Page 18
APPENDIX A Terms and Definitions	Page 19
APPENDIX B Federal Laws Relevant To Seeking, Retaining, and and Disseminating Justice Information	Page 28

Purpose Statement

The purpose of this policy is to establish privacy guidelines for the Western Pennsylvania All Hazards Fusion Center (WPAHFC). The W P A H F C is an information sharing and analysis center with an all threats and all hazards approach through the collation, analysis, and dissemination of intelligence and investigative information within the fourteen county area of Southwestern Pennsylvania. The Center is not intended to supplant the activities of the numerous investigative and operational bodies currently functioning in these counties, but will provide them with an additional tool to be more effective and focused in their tasks while ensuring protection of the legal rights and privacy of its citizens.

Policy Applicability and Legal Compliance

1. All WPAHFC personnel (law enforcement, public, private sector, contractors and other authorized users with direct access to WPAHFC information), will comply with this privacy policy and with 18 Pa C.S. §9106, the Commonwealth of Pennsylvania Right to Know Law (Act 3 of 2008), the constitutions of the United States and the Commonwealth of Pennsylvania, and the applicable law protecting privacy, civil rights and civil liberties in the collection, use, analysis, retention, destruction, sharing and disclosure of information. Title 28 CFR Part 23 shall be adhered to in the situations wherein it is applicable.
2. It is WPAHFC internal operating policy to comply with applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing and disclosure of information in the WPAHFC information system. All information provided by WPAHFC from outside sources must be verified from those sources if the information is to be used in an investigative capacity.
3. All participating WPAHFC personnel, personnel providing information technology services to WPAHFC, private contractors, governmental agencies including Information Sharing Environment (ISE) participating agencies and centers, and users will comply with the applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information received from the WPAHFC. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies including ISE participating agencies and centers, and participating justice and public safety agencies, as well as private contractors, private entities, and the general public. Agencies receiving intelligence, investigative, or treatment information as defined in 18 Pa C.S. §9102 must submit appropriate policies and procedures for dissemination of protected information as mandated in 18 Pa C.S. §9106(c).

Transparency and Accountability

1. A steering committee known as the WPAHFC Steering Committee (WSC) has been established. The WSC will provide advice and guidance to the Director of the WPAHFC regarding the direction and priorities of WPAHFC and establish policies and procedures governing WPAHFC operations including the protection of privacy, civil rights, and civil liberties. The WSC is comprised of a single representative designated by the Region 13 Board of Directors, a single representative designated by the Director of the City of Pittsburgh Department of Public Safety, A single representative designated by the Commissioner of the Pennsylvania

State Police, and a single representative designated by the Special Agent in Charge of the FBI Pittsburgh Division. The WSC in conjunction with the PA REGION 13 TASK FORCE Board of Directors acts as the decision-making body for the PA REGION 13 FUSION CENTER. The PA REGION 13 TASK FORCE Board of Directors is made up of the 14 Emergency Management Coordinators that represent the 13 Counties, and the City of Pittsburgh, that comprise the PA Region 13 Task force. The WSC appoints the PA Region 13 Fusion Center staff, including the Fusion Center Director. The PA REGION 13 TASK FORCE Board of Directors will serve as the designated privacy oversight committee that liaises with the community to ensure that privacy and civil rights are protected as provided in this policy and by the center's information-gathering and collection, retention, and dissemination processes and procedures. The Board will annually review and update the policy in response to changes in law and implementation experience, including the results of audits and inspections.

2. The WPAHFC Fusion Center Director has the primary responsibility for the operation of the W P A H F C , operations, and coordination of personnel; the receiving, seeking, retention, and evaluation of information; information quality, analysis, destruction, sharing, or disclosure; and the enforcement of this policy.

3. The WPAHFC personnel will follow 18 Pa C.S. §9106, and other laws as enacted by the Pennsylvania Legislature and signed by the Governor pertaining to the collection, collation, use, analysis, retention, destruction, sharing, and disclosure of intelligence information, archived information, and investigative information.

4. The WPAHFC Fusion Center Director appoints a Privacy Officer who will receive appropriate training. 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: Western Pennsylvania All Hazards Fusion Center, ATTN: Privacy Officer, 800 Cranberry Woods Drive, Suite 250, Cranberry Township, PA 16066. Complaints can also be received by the WPAHFC Privacy Officer via telephone at 724-778-8801.

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

Information

1. The WPAHFC's intelligence and investigative information is received from, and disseminated to, local, state, federal, and tribal law enforcement; other Fusion Centers; the public; and private entities, as appropriate and in compliance with 18 Pa C.S. §9106.

2. The WPAHFC will seek or retain information that:

- Is based on a criminal predicate or threat to public safety; or
- Is based on reasonable suspicion that an individual or group has committed a criminal offense

or is involved in, and/or planning, criminal (including terrorist) conduct or activity that presents a threat to any individual, community, or the nation, and that the information is relevant to the criminal (including terrorist) conduct or activity where such criminal activity would give rise to prosecution for a state offense graded a misdemeanor or felony or for a federal offense for which the penalty is imprisonment for more than one year; or

- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, and sentences; or the prevention of crime; or
- Is useful in crime analysis, or in the administration of criminal justice and public safety (including topical searches); and
- The source of the information is reliable and verifiable, and/or limitations on the quality of the information are identified; and
- The information was collected in a fair and lawful manner not otherwise prohibited by law, with the consent of the affected individual to share the information being clearly noted when such consent has been provided.

3. All PA REGION 13 FUSION CENTER information will be sought, retained, shared, or disclosed under the appropriate policy provisions.

4. The WPAHFC will not seek or retain, 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, or sexual orientation.

5. The WPAHFC may retain information that is based on a level of suspicion that is less than reasonable suspicion, such as tips, leads, and Suspicious Activity Report (SAR) information, subject to the policies and procedures outlined in this policy.

6. The WPAHFC requires certain basic descriptive information to be entered and electronically associated with data (or content), including SARs and terrorism-related SARs (ISE-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 conforms to WPAHFC submission standards.
- Any particular limitations to the use or disclosure of the information.

7. Upon the receipt of information, WPAHFC personnel will evaluate the information to determine its nature, usability, and quality. Personnel will assess information to ensure proper segregation and categorization, including the level of protection to be afforded the information based upon the type of information received (based on sensitivity or classification) and to what extent it may be shared through the ISE, to reflect the assessment, such as:

- Whether the information is based upon a standard of reasonable suspicion of criminal activity;
- Whether the information is general data, tips and leads, SAR or criminal intelligence information
- The nature of the source (i.e. anonymous tip, interview, public or private sector)
- The reliability of the source:
 - Reliable – 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 cannot be judged or assessed.
- The validity of the content is confirmed, doubtful or cannot be judged.

8. At the time a decision is made by WPAHFC to retain information, it will be categorized regarding the type of information (tips/leads, SARs, criminal intelligence information, etc.), nature of the source, reliability of the source, and sensitivity of the information (including the application of labels and/or metadata tags) pursuant to applicable limitations on access and sensitivity of disclosure in order to:

- Protect confidential sources and law enforcement undercover techniques and methods;
- Prevent interference with or compromise pending criminal or terrorism investigations;
- Protect an individual's right of privacy, civil rights, and civil liberties; and
- Provide legally required protection based on the individual's status, such as in the case of a juvenile.

9. The classification of existing information will be reevaluated whenever:

- New information is gathered that has an impact on the validity and reliability of the retained information;
- There is a change in the use of the information affecting access or disclosure limitations;
- Per scheduled retention reviews.

10. WPAHFC personnel, partners and participating agencies will be required to adhere to specific practices and procedures for the receipt, collection, assessment, marking, storage, access, dissemination, retention, and security of tips and leads, and SAR/ISE-SAR information.

WPAHFC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. Center personnel will:

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.
- Store the information using the same storage method used for data which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, “need-to-know” and “right-to-know” access or dissemination for personally identifiable information).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain information for up to two years in order to investigate an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the center’s physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

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

12. For purposes of sharing information in the Information Sharing Environment, the WPAHFC will identify all terrorism-related information (via notice mechanisms, including metadata and/or data field labels) thus enabling users to determine the nature of the information along with the enhanced privacy protections for such information as are specified in this policy.

13. The WPAHFC will track assessment and dissemination to clearly indicate any legal restrictions on information sharing based on information sensitivity, nature of protected information, or classification.

14. The WPAHFC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- The information is protected information to include personal information on any individual [See Terms and Definitions], and, to the extent expressly provided in this policy, includes organizational entities.
- The information is subject to the laws cited in the Policy Applicability and Legal Compliance restricting access, use, or disclosure.

15. The WPAHFC will keep a record of the source of all information sought and collected by the center.

Acquiring and Receiving Information

1. Information gathering and investigative techniques used by the WPAHFC and participating agencies will comply and adhere to regulations and guidelines including, but not limited to:

- Federal (see Appendix B) and state laws (see Policy Applicability and Legal Compliance) and constitutional guarantees protecting privacy, civil rights and civil liberties or citizens, the Bill of Rights amendments to the U.S. Constitution, the Declaration of Rights to the Pennsylvania Constitution and the Pennsylvania Human Relations Act and the Federal Civil Rights Act;
- 28 CFR Part 23 regarding criminal intelligence information;
- Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).

2. 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 WPAHFC systems or submitted to or received by the WPAHFC.

3. Agencies which participate and provide information to the WPAHFC are governed by state and local laws and rules governing them, as well as by applicable federal laws. The WPAHFC 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 which is not based on misleading information collection practices.

4. The WPAHFC will not directly or indirectly receive, seek, accept or retain information from:

- An individual or non-governmental 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

- A source that used prohibited means to gather the information.

5. Law enforcement officers and personnel at source agencies who acquire SAR information that may be shared with the WPAHFC will be trained to recognize behavior that is indicative of criminal activity related to terrorism (including human review and vetting of the information). The responsibility for this training resides with the contributing agency.

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

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

Information Quality

1. To the maximum extent practical, the WPAHFC 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 information for accuracy) do not apply to an intelligence-gathering initiative. All contributors of information to the WPAHFC 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 the WPAHFC.

2. The WPAHFC will make every reasonable effort to ensure that information sought or retained, to include SAR information, is derived from dependable and trustworthy sources; accurate, current, and complete, ensuring the relevant context in which it was sought or received; and merged with other information when applicable standard [Merging Information from Different Sources] has been met.

3. At the time of retention in the system, the information will be labeled in regards to its level of quality (current, accurate, complete, verifiable, and reliable). The WPAHFC investigates, in a timely manner, alleged errors and deficiencies, and corrects, deletes, or refrains from using protected information found to be erroneous or deficient. The retained information will be reevaluated when new information is received that has an impact on the confidence (content validity and source reliability) of the previously retained information.

4. The WPAHFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard (refer to Merging of Information from Different Sources) has been met. The center will conduct periodic data quality reviews of the information it originates and will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used upon learning that such information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the agency; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

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

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

Collation and Analysis

1. Information acquired or received by the WPAHFC, or accessed from other sources, will be analyzed only by qualified individuals who have successfully completed a background check and retain appropriate security clearance, if applicable, and who have been selected, approved, and trained accordingly. WPAHFC personnel will comply with laws regarding privacy, civil rights, and civil liberties.

2. Information acquired or received by the WPAHFC, or accessed from other sources, is analyzed according to priorities and needs only to:

- Further crime prevention (including terrorism), law enforcement, force deployment, public safety or prosecution objectives and priorities established by the WPAHFC.
- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in, or engaging in criminal or terrorist activities.

3. Information subject to collation and analysis is information as defined and identified in [Refer to Information].

4. WPAHFC requires that all analytical products be reviewed and approved by the Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

Merging of Information from Different Sources

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 a match.

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

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.

Sharing and Disclosure

1. Information retained by the WPAHFC will only be provided to persons within the criminal justice system who are authorized to receive the information and only for legitimate law enforcement, public prosecution, public protection, public health, or justice purposes.

2. Intelligence information placed in an automated information system may only be disseminated if: (a) the information is reliable as determined by an authorized intelligence officer; (b) the agency requesting the information is a criminal justice agency which has policies and procedures consistent with 18 Pa C.S. §9106; and (c) the information requested is in connection with the duties of the criminal justice agency and the request is based on specific identifying information. Agencies external to the center may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

3. Information retained by the WPAHFC may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.

4. Information possessed by WPAHFC that is considered nonpublic record information will only be disclosed to an individual as the result of the issuance of a proper Subpoena Duces Tecum or, if the subpoena is objected to, a subsequent court order. If information gathered or collected and records retained by the WPAHFC 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 otherwise appropriate for release to further the center'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 center 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.

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

- Records required to be kept confidential by law are exempted from disclosure requirements under Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008;
- Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606;
- Investigatory records of law enforcement agencies that are exempted from disclosure requirements under Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008. However, certain law enforcement records must be made available for inspection and copying under Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008;
- 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 Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008. This includes a record maintained by an agency in connection with the military, homeland security, national defense, law enforcement or other public safety activity that if disclosed would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity or a record that is designated classified by an appropriate federal or state military authority;
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under 18 Pa C.S. §9106, be shared without permission;
- A violation of an authorized nondisclosure agreement under 18 Pa C.S. §9106.

6. An audit trail sufficient to allow the identification of each individual who accessed information or received information retained by WPAHFC and the nature of the information accessed will be kept by WPAHFC.

7. WPAHFC will adhere to the current version of the ISE-SAR Functional Standard for the reporting of suspicious activity in the ISE, 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.

8. Credentialed, role-based access criteria will be used by the WPAHFHC, as appropriate, to control:

- The information to which a particular group or class of users can have access based on the group or class.
- The information a class of users can add, change, delete, or print.
- To whom, individually, the information can be disclosed and under what circumstances.

9. Information gathered or collected and records retained by the WPAHFHC 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 for a minimum of two years by the center.

10. The WPAHFHC 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.

Redress

1. Upon submission of and approval of a Pennsylvania Right to Know Law Request and satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in 2., below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the W P A H F C . The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). 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.

2. The existence, nonexistence, content, and source of the information will not be made available by the WPAHFHC to an individual when:

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008) (refer to Attachment 3);
- Disclosure would endanger the health or safety of an individual, organization, or community (Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008);
- The information is in a criminal information system subject to 28 CFR Part 23 and 18 Pa C.S. §9106;

- The information source does not reside with the WPAHFC or WPAHFC did not originate and does not have a right to disclose the information (18 Pa C.S. §9106).

If the information did not originate in the WPAHFC, the source agency will be notified and a request for its determination that disclosure by WPAHFC or referral of WPAHFC to the source agency was neither required nor appropriate.

3. If an individual requests correction of information **originating with the WPAHFC** that has been disclosed, the center's Privacy Officer will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

4. The individual who has requested disclosure will be given reasons if disclosure or requests for corrections are denied by WPAHFC. The individual will also be informed of the procedure for appeal per the Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008 when WPAHFC has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

5. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that: (a) is exempt from disclosure, (b) has been or may be shared through the ISE, (1) is held by WPAHFC and (2) allegedly has resulted in demonstrable harm to the complainant, WPAHFC will inform the individual of the procedure for submitting and resolving such complaints. Complaints can be sent by mail to the center's Privacy Officer at the following address: Western PA All Hazards Fusion Center, Attention: Fusion Center Privacy Officer, 800 Cranberry Woods Dr. Cranberry Township, PA 16066. Complaints can also be received by the WPAHFC Privacy Officer via telephone at (724) 778-8801. The Privacy Officer will refer the complaint to the Board of Directors, where it will be reviewed and if necessary, referred to legal counsel. The Privacy Officer will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 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. All information held by WPAHFC that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, WPAHFC will not share the information until such time as the complaint has been resolved. A record will be kept by WPAHFC of all complaints and the resulting action taken in response to the complaint.

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

Information Retention and Destruction

1. Criminal intelligence information and SARs retained by the WPAHFC will be reviewed for purging at least every five years. Other information and intelligence will be reviewed as established by 18 Pa C.S. §9106. When information has no further value or meets the criteria for removal under Pa C.S. §9106 and 28 CFR Part 23 (for criminal intelligence information), it will be purged, destroyed, deleted, or returned to the submitting source. Notification that information is subject to purging if not reviewed and validated will be provided 30 days prior to the required review and validation/purge date. The purging or removal of data shall be approved by a supervisor in accordance with applicable WPAHFC administrative regulations. No approval will be required from the originating agency before information held by the WPAHFC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

2. According to 18 Pa C.S. §9106, WPAHFC will purge intelligence information under the following conditions: (a) the data is no longer relevant or necessary to the goals and objectives of the WPAHFC; (b) the data has become obsolete, making it unreliable for present purposes and the utility of updating the data would be worthless, or (c) the data cannot be utilized for strategic or tactical intelligence studies.

Accountability and Enforcement

1. The policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public on request and through the PA REGION 13 TASK FORCE public website at www.pa-region13.org.

2. The 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. The Privacy Officer and the Board of Directors shall receive training in the protection of privacy, civil rights, and civil liberties. The Board of Directors point of contact is the WPAHFC Fusion Center Privacy Officer, who can be contacted by phone at (724) 778-8801. Additionally, external inquiries and complaints can be directed to the Board of Directors through the WPAHFC. The Privacy Officer can be contacted by phone at (724) 778-8801. Any complaints or reports of violations of department policies by WPAHFC personnel will be handled through appropriate internal WPAHFC policies and procedures. Inquiries or complaints that are received by the Board of Directors involving non-WPAHFC personnel will be directed to the Fusion Center Director who will report the matter to the employee's agency. Information received by the WPAHFC pertaining to civil rights or civil liberties will be immediately forwarded to the Privacy Committee for consideration and/or action.

3. Center personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the WPAHFC Director. The WPAHFC Director is responsible for handling any errors or violations with regard to this policy. The designated WPAHFC Security Officer shall receive appropriate training regarding the safeguarding and security of information. The Fusion Center Director shall report all errors or violations of this policy to the WPAHFC Steering Committee.
4. WPAHFC will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall comply with security requirements outlined in 18 Pa C.S. §9106.
5. WPAHFC will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23 and 18 Pa C.S. §9106.
6. WPAHFC will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions as provided in WPAHFC regulations.
7. WPAHFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the system itself 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 WPAHFC Director.
8. WPAHFC will at least annually conduct audits and inspections of the information contained in the justice information system. The audits will be conducted randomly, without announcement, at any time, and without prior notice to staff at the center, by a designated representative of the WPAHFC or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of information.
9. WPAHFC will require any individuals authorized to use the system to acknowledge receipt of the policy and agree to comply with the provisions of this policy in writing. A copy of the policy, in a printed format, will be made available to all individuals authorized to use the system.
10. WPAHFC reserves the right to restrict the qualifications and number of personnel having access to WPAHFC information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the WPAHFC's privacy policy.

11. The WSC will annually review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations. This document can be altered and expanded as the ISE and other sharing systems are defined and implemented.

12. If a user is suspected of or found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, WPAHFC will: (a) suspend or discontinue access to information by the user; (b) suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies; (c) apply other sanctions or administrative actions as provided in agency personnel policies; (d) request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or (e) refer the matter to appropriate authorities for criminal prosecution, as necessary.

13. In compliance with Pennsylvania's Breach of Personal Information Notification Act, WPAHFC will notify individuals if their personal information is compromised by a breach of computer security.

14. Access to WPAHFC 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.

15. Queries made to the WPAHFC's data applications will be logged into the data system identifying the user initiating the query.

16. The WPAHFC will utilize watch logs to maintain audit trails of requested and disseminated information.

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

Training

1. The WPAHFC will require annual training for the following individuals regarding implementation of and adherence to the privacy policy:

- Any person that is granted direct access to WPAHFC information (including personnel providing information technology services to the center, board of directors, private contractors and staff in other agencies providing services to the center).
- Personnel authorized to share protected information through the Information Sharing Environment.

2. The WPAHFC's privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection policy;
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the WPAHFC;
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
- The impact of improper activities associated with infractions within, or through, the agency;
- Originating and participating agency responsibilities and obligations under applicable law and policy;
- Mechanisms for reporting violations of WPAHFC privacy-protection policies; and
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

Sharing of Information Among Participants

1. Participating agencies with a memorandum of understanding or policies and procedures will conduct periodic data quality reviews and adopt internal policies and procedures requiring the participating agency, its personnel, contractors, and users to: (a) only seek or retain information that is legally permissible for the agency to seek or retain under laws applicable to the agency; (b) only use lawful means to seek information; (c) only seek and retain information that is reliably accurate, current, and complete, including the complete, relevant context; (d) take appropriate steps when merging information about an individual or organization from two or more sources to ensure that the information is about the same individual or organization and is referenced as to the source; (e) investigate in a timely manner any alleged errors and correct or delete information found to be erroneous; (f) retain information sought or received only so long as it is relevant and timely, and delete or return information that is inaccurate, outdated, or otherwise no longer related to known or suspected criminal, including terrorist, activities; (g) maintain information and systems containing information in a physically and electronically secure environment and protected from natural or man-made disasters or intrusions; (h) engage in collation and analysis of information in a manner that conforms to generally accepted practices; (i) establish procedures that comply with the policies and procedures of the justice information sharing system for accessing information through the participating agency; (j) only allow authorized users to access the information in the shared system and only for purposes related to the performance of their official duties; (k) share information with authorized users of other justice system partners based only on a “right-to-know” and a “need-to-know” basis; and (l) establish and comply with information retention and destruction schedules.

2. Information obtained from WPAHFC will not be used or publicly disclosed for purposes other than those specified in the memorandum of understanding. Information cannot be sold, published, exchanged, or disclosed for commercial purposes; disclosed or published without prior approval of the contributing agency; or disseminated to unauthorized persons.

Use and Disclosure of Information Originating from Another Participating Agency

1. A participating agency will not disclose information originating from another agency except as authorized or required by law in the jurisdiction in which the information originated or by following the third-party dissemination rule.
2. When a participating agency gathers or receives information that suggests that information originating from another agency may be erroneous, may include incorrectly merged information, or lacks relevant context, the alleged error will be communicated in writing to the person designated in the originating agency to receive such alleged errors.

Appendix A

Terms and Definitions

Access—Data access refers to the ability to get to (usually having permission to use) particular data on a computer. Web access refers to 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 or read/write access.

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

Access Control—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 Information Sharing Environment participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer to the obtaining of information widely available to other Information Sharing Environment participants, for example, through news reports or by obtaining information from another Information Sharing Environment participant who originally acquired the information.

Agency—Agency refers to the Western Pennsylvania All Hazards Fusion Center (WPAHFC) and all agencies that access, contribute, and share information in the WPAHFC's justice information system.

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

Audit trails are a fundamental part of computer security and are 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 provides adequate credentials that prove identity. 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 access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access, and that is verified through authentication. *See Authentication.*

Authorized User—A person that is granted direct access to WPAHFC information.

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. Implementations of the latter include voiceprints and handwritten signatures.

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

Civil Rights—The term “civil rights” is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual; therefore civil rights are 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—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 used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal Intelligence Information or Data—Information deemed relevant to the identification of, and the criminal activity engaged in, by an individual 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.

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

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

Data Protection—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, for example 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.

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

The eight FIPs are:

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

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

General Information or Data—Information that may include records, documents, or files pertaining to law enforcement operations such as computer-aided dispatch (CAD) data, incident data, and management information; and 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—Since a privacy policy is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the policy.

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

Information Quality—Information quality refers to various aspects of the information such as 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 (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).

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*.

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

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

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

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

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

Persons—Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency considered 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—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 written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection— 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—Protected information includes Personal Data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Pennsylvania constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; and applicable state and local laws and ordinances. Protection may also be extended to organizations by center policy or state or local law.

Public—Public includes:

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

Public does not include:

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

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—Laws, policies, and Internal procedures to 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 that is under the center's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

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

Retention—*Refer to Storage.*

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

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

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

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

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

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

Suspicious Activity Report (SAR)—Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to

be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

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

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

Tips and Leads Information or Data—Uncorroborated reports 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. Tips and leads information is 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 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 falls between being of no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

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

Appendix B

Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Excerpt from

*U.S. Department of Justice's (DOJ's) Privacy, Civil Rights, and Civil Liberties
Policy Templates for Justice Information Systems*

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, and tribal (SLT) agencies. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution but can (and many do) provide enhanced privacy and other civil liberties protections.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the Information Sharing Environment is explored in a key issues guidance paper titled *Civil Rights and Civil Liberties Protection*, which is available on the Program Manager (PM) for the Information Sharing Environment (PM-ISE) Web site at www.ise.gov.

Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Persons Act.

Federal laws, Executive Orders, regulations, and policies directly affect agencies'/centers' privacy policies. While SLT agencies may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., 28 CFR Parts 20, 22, and 23 or the Health Insurance Portability and Accountability Act [HIPAA]); operation of the Commerce Clause of the U.S. Constitution (e.g., Electronic Communications Privacy Act of 1986); or a binding agreement between a federal agency and an SLT agency (e.g., a memorandum of agreement or memorandum of understanding). Where relevant or possibly relevant, agencies/centers are advised to list these laws, regulations, and policies, noting those that may potentially affect the sharing of information, including sharing terrorism-related information in the Information Sharing Environment.

The development of a privacy, civil rights, and civil liberties policy is primarily designed for center personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the center must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an center privacy policy, staff and user accountability is greatly diminished, mistakes are made, privacy violations occur, and the public's (and other agencies') confidence in the ability of the center to protect information and intelligence is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, information sharing is enhanced.

Following is a partial listing of federal laws that should be reviewed when developing a privacy policy for a justice information system. The list is arranged in alphabetical order by popular name.

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

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data—Protecting Personal Privacy," December 20, 2000

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