# West Virginia Intelligence/Fusion Center

# Privacy Policy

**Final Draft: February 25, 2011**

## A. Purpose Statement

The West Virginia Intelligence/Fusion Center (WVI/FC) was stood up in its present form on March 17, 2008, and was established within the West Virginia Department of Military Affairs and Public Safety by Governor Joe Manchin III, to detect, prevent, vet, and respond to information concerning criminal and terrorist activities and all other crimes and hazards that might affect the safety and wellbeing of the people and the property of the State of West Virginia, her visitors and guests. The mission of the WVI/FC is:

The WVI/FC is a partnership between public and private entities. Through the cooperation of local, state, and federal law enforcement, public safety agencies, and the private sector, the Fusion Center is able to better protect the citizens of West Virginia and the citizens of the United States against all-crimes and all-hazards. This is accomplished by aggressively facilitating the collection and compilation of all credible information and, through professional analysis of collected information and open source documents, by producing reliable and credible intelligence. The Mission of the Fusion Center is then to anticipate, identify, prevent, and monitor criminal activity and all other hazards and to responsibly distribute that intelligence to its stakeholders while both protecting the privacy rights and civil liberties of its citizens and guarding the rights and integrity of law enforcement and private industry.

WVI/FC's Privacy Policy applies to all individuals and all organizations and is in compliance with Executive Order No. 6-06, August 16, 2006 (See http://www.privacy.wv.gov/privacy-program/Documents/Executive_Order_No__6-06.pdf), and 28 Code of Federal Regulations (CFR) Part 23. The purpose of WVI/FC's Privacy Policy is to ensure that WVI/FC personnel with direct access to WVI/FC information comply with federal, state, local, and tribal law, WVI/FC's policies and procedures, and assists its authorized users in:

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

- Minimizing reluctance of individuals or groups to use or cooperate with the justice system;
- Supporting the role of the justice system in society;
- Promoting governmental legitimacy and accountability;
- Not unduly burdening the ongoing business of the justice system; and
- Making the most effective use of public resources allocated to public safety agencies.

**B. Policy Applicability and Legal Compliance**

All WVI/FC personnel, personnel who provide information technology services to the WVI/FC, and private contractors with direct access to WVI/FC information, will comply with the WVI/FC's privacy policy concerning the information the WVI/FC collects, receives, maintains, archives, accesses, or discloses to WVI/FC personnel, governmental agencies, including agencies participating in the Information Sharing Environment, participating law enforcement agencies, and participating justice and public safety agencies, as well as to private contractors and the general public.

The WVI/FC will provide a printed copy of this policy to all personnel who are assigned to the WVI/FC and have direct access to WVI/FC information and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

All WVI/FC personnel with direct access to WVI/FC information, other law enforcement agencies, and private contractors with access to WVI/FC information and who provide information technology services to the WVI/FC shall comply with applicable law protecting privacy, civil rights, and civil liberties which includes, but which is not limited to, the U.S. and West Virginia constitutions, Executive Order No. 6-06, August 16, 2006, the West Virginia Freedom of Information Act, Chapter 29B-1-1 et seq., the West Virginia Sunshine Act, Chapter 6-9A-1 et seq., and applicable Federal law (See Appendix B), including 28 Code of Federal Regulations (CFR) Part 23.

The WVI/FC has adopted internal operating policies and procedures that are in compliance with the applicable law protecting privacy, civil rights, and civil liberties cited above.

**C. Governance and Oversight**

Primary responsibility for the operation of the WVI/FC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the Director of the WVI/FC.

The Director of the WVI/FC will create an Oversight Committee (hereinafter the Committee) for WVI/FC to provide strategic direction, ensure objectives are achieved, risks are managed appropriately, and resources are used responsibly. This Committee will meet regularly to provide input due to the collaborative nature of the WVI/FC.

The Committee will liaise with the community to ensure that privacy, civil rights, and civil liberties are protected as provided within the provisions of this policy and by the WVI/FC's information-gathering and collection, retention, and dissemination processes and procedures. The Committee will review the policy at least annually and recommend updates, as appropriate, to the Director in response to changes in law and implementation experience, including the results of audits and inspections.

The WVI/FC Deputy Director will be properly trained to serve as the Privacy Officer and will receive reports regarding alleged errors and violations of the provisions of this policy and receive and coordinate compliant resolution under the Fusion Center's redress policy. The Privacy Officer is responsible for the direct oversight of the privacy policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information and thus is responsible for notifying the Director of the WVI/FC regarding noncompliance issues. The Privacy Officer ensures that enforcement procedures and sanctions outlined in Section N.3., Enforcement, are adequate and enforced.

The Privacy Officer also serves as the liaison for the Information Sharing Environment (ISE), 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 e-mail address: wvfusion@wv.gov, Attention: WVI/FC Privacy Officer.

**D. Definitions**

Primary terms and definitions used in the WVI/FC Privacy Policy are located in Appendix A.

**E. Information**

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

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

- Is based on a criminal predicate or threat to public safety; or

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

• Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders of sentences; or the prevention of crime; or

• Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); and

• The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and

• The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

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

The WVI/FC may retain protected information that is based on a level of suspicion that is less than reasonable suspicion, such as tips and leads. Suspicious Activity Report (SAR) information will be retained and processed in accordance with the current version of the ISE-SAR Functional Standard, (ISE-SAR FS). Tips and leads and SAR information will be labeled and maintained separately from other WVI/FC information databases. ISE-SAR information will be identified and maintained in a WVI/FC shared space under the ISE-SAR FS.

The WVI/FC will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

The WVI/FC 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 as defined by the center to include personal information on any individual [see definitions of "protected information" and "personal information" in Appendix A of policy], and, to the extent expressly provided in this policy, includes organizational entities.

- The information is subject to local, state or federal law (see Appendix B) restricting access, use, or disclosure.

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

- Whether the information is based upon a standard of reasonable suspicion of criminal activity;

- Whether the information consists of tips and leads data or suspicious activity reports;

- The nature of the source as it affects veracity (for example, anonymous tips, trained interviewer or investigator, public record, private sector); and

- The validity of the content (for example, verified, partially verified, unverified, or unable to verify).

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

- Protect confidential sources and law enforcement undercover techniques and methods;

- Not interfere with or compromise pending criminal or terrorism investigations;

- Protect an individual's right of privacy, civil rights, and civil liberties; and

- Provide legally required protection based on the individual's status such as a juvenile.

The classification of existing information will be re-evaluated whenever:

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or

- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

WVI/FC 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 five years in order to work an invalidated 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.

The WVI/FC 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 information privacy, civil rights, and civil liberties.

The WVI/FC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the ISE. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels, which 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.

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

• The name of the originating center, department or agency, component, and subcomponent.

• The name of the center's justice information system from which the information is disseminated.

• The date the information was collected and, where feasible, the date its accuracy was last verified.

• The title and contact information for the person to whom questions regarding the information should be directed.

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

The WVI/FC will keep a record of the source of all information sought and collected by the center.

**F. Acquiring and Receiving Information**

Information-gathering (acquisition) and access and investigative techniques used by the WVI/FC and information-originating agencies will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:

• 28 CFR Part 23, regarding criminal intelligence information.

• The OECD Fair Information Principles.

• Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).

• U.S. and West Virginia constitutional provisions; applicable West Virginia State Code provisions cited in Section B, Paragraph 3, above, and administrative rules and orders, including EO 6-06 (April 16, 2006), as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

The WVI/FC'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 safety, law enforcement or 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 these threats.

The WVI/FC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals or organizations involved in activities that have been determined to be consistent with criminal activities associated with terrorism, safety, and

criminal activities will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

Information-gathering and investigative techniques used by the WFI/FC will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

External agencies that access/receive the WVF/IC'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.

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

The WVF/IC will not directly or indirectly receive, seek, accept, or retain information from:

- An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy – such as a paid informant.

- An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

**G. Information Quality Assurance**

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

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

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

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

The WVI/FC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that information will be corrected, deleted from the system, or

not used when the WVI/FC learns that the information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the agency; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

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

The WVI/FC will use written or documented electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the WVI/FC 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.

**H. Collation and Analysis**

Information acquired or received by the WVI/FC, or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly, or under the direct supervision of the Watch Center Supervisor.

Information subject to collation and analysis is information as defined and identified in Section E, Information.

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

- Further crime prevention (including terrorism), law enforcement, force deployment, or prosecution objectives and priorities established by the WVI/FC, or

- 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, or

- To prevent or assist in the health and wellbeing of the citizens of West Virginia or persons visiting or passing through this state.

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

## I. Merging Records

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

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

## J. Sharing and Disclosure

Access to WVI/FC information:

- The Director of the WVI/FC, and/or administrator(s) designated by the Director, shall establish requirements and record all personnel as to their access authority and permission to access WVI/FC's information;

- Permission's regarding viewing, adding, editing and printing of WVI/FC information is controlled by WVI/FC's administrator(s) on all WVI/FC's information;

- All WVI/FC personnel, with approval from the Director, or his/her designee, may disclose WVI/FC information pursuant to applicable policy;

- An audit trail shall be maintained regarding access to, and disclosure of, WVI/FC information.

The WVI/FC 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.

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

Agencies external to the WVI/FC may not disseminate WVI/FC information received from WVI/FC without approval from the originator of the information.

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

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

Information gathered and records retained by the WVI/FC 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 WVI/FC 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 WVI/FC for this type of information or when there is a legitimate need. Requests of this nature are recorded in the Watch Center Call Log Information Sheet. The request and any information disclosed are recorded in the Watch Center Call Log Information Sheet.

Information gathered and records retained by the WVI/FC will not be:

> • Sold, published, exchanged, or disclosed for commercial purposes except that this section will not forbid the Director from using non-private information or parts of reports or occurrences for the education of the public as to the WVI/FC's mission, accomplishments, and activities so long as doing so does not violate any of the privacy concerns of this document; State, Local, Federal, or Tribal laws, or the WVI/FC's policy and procedures; or
>
> • Disclosed or published without prior notice to the originating agency that such information is subject to re-disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency; or
>
> • Disseminated to persons not authorized to access or use the information.

There are several categories of otherwise public records that will ordinarily not be provided to the public by the WVI/FC under relevant provisions of §29B-1-4 Exemptions, of the West Virginia Freedom of Information Act, including:

- Information of a personal nature such as that kept in a personal, medical, or similar file, if the public disclosure thereof would constitute an unreasonable invasion of privacy, unless: (1) the public interest by clear and convincing evidence requires disclosure in the

particular instance; or (2) an individual is requesting his or her personal file. (Exemption 2);

- Law enforcement records that deal with the detection and investigation of crime and internal records and notations which are maintained for internal use in matters related to law enforcement. (Exemption 4);
- Information specifically exempted from disclosure by statute. (Exemption 5);
- Internal memoranda or letters received or prepared by any public body. (Exemption8);
- Homeland security information, including but not limited to, certain records related to preventing mitigating, or responding to a terrorist attack, vulnerability assessments, certain intelligence and investigative records, classified national security information under Presidential Executive Order 13549, August 18, 2010, and federal law, and disaster recovery plans. Exemptions 9 – 18).

The WVI/FC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

**K. Redress**

**K.1 Disclosure**

Upon satisfactory verification, which may include fingerprints, driver's license, and/or other specified identifying documentation of his or her identity and subject to the conditions specified 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 WVI/FC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction).

Requests for disclosure of WVI/FC records by the public will be handled according to established procedures under West Virginia Freedom of Information Act §29B-1-1 et seq. The WVI/FC's response to the request for information will be made within a maximum of 5 days, not including Saturdays, Sundays, or legal holidays, as provided under §29B-1-3(4) of the West Virginia Freedom of Information Act, and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

The existence, content, and source of the information will not be made available to an individual when the information is determined not to be a "public record" under §29B-1-2(4) or to be exempt from disclosure under §29B-1-4 of the West Virginia Freedom of Information Act.

If the information did not originate with WVI/FC, the requestor will be referred to the originating agency, if appropriate or required or for basic information requests not associated with individual corrections or complaints, or the center will notify the source agency of the request and its determination that disclosure by the center or referral of the requestor to the source agency was neither required nor appropriate under applicable law. As appropriate, WVI/FC will coordinate with the source agency, lending any assistance available to ensure that the individual is provided with applicable complaint submission or corrections procedures and by either eliminating incorrect information from the WVI/FC records and/or assisting the originating agency to do the

same. A record will be kept of all such complaints and request for corrections, and the resulting action taken, if any.

**K.2 Complaints and Corrections**

If an individual has complaints or objections to the accuracy or completeness of information about him or her originating from WVI/FC information that has been disclosed, the WVI/FC will inform the individual of the procedure for requesting and considering corrections. If an individual's complaint or objection cannot be resolved after initial review by the WVI/FC Privacy Officer, the individual may request a review of that decision by the Director. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

**K.3 Redress**

If an individual has a complaint with regard to the accuracy or completeness of protected information that:
(a) Is exempt from disclosure,
(b) Has been or may be shared through the ISE,
    (1) Is held by the WVI/FC, and
    (2) Allegedly has resulted in demonstrable harm to the complainant,
The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer at wvfusion@wv.gov, Attention: WVI/FC Privacy Officer. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but 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 the center that is the subject of a redress 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, the center will not share the information until such time as the complaint has been resolved
A record will be kept of all complaints and requests for corrections, and the resulting actions, if any.

To delineate protected information shared through the ISE from other data, the WVI/FC maintains records of agencies sharing protected information and employs system mechanisms to identify the originating agency when the information is shared.

**L. Security Safeguards**

The WVI/FC's Fusion Center Deputy Director is designated and trained to serve as the WVI/FC's Security Officer.

The WVI/FC is located within a secure facility, thus protected from external intrusion. The WVI/FC's office space is only accessible to WVI/FC personnel and other personnel that have

been issued an access card for the WVI/FC or under the direct control and supervision of an authorized WVI/FC participant. The WVI/FC will utilize secure internal and external safeguards against network intrusions. Access to WVI/FC systems from outside the facility will be allowed only over secure networks. The WVI/FC's information system is a West Virginia Office of Technology system and thus maintained by them. All WVI/FC systems are required to complete an annual security risk assessment to identify vulnerabilities.

The WVI/FC will label tips and leads and SAR information. The WVI/FC 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.

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

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

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

The WVI/FC utilizes' the Watch Center Call Log Information Sheet to record requested and disseminated information.

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

The WVI/FC 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 of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

**M. Information Retention and Destruction**

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

The WVI/FC will delete information, or return it to the source, as required in 28 CFR Part 23 and as provided in source agency participation agreements.

A revised policy for the retention and destruction of tips/leads and SARs information will be determined by the Oversight Committee and included in a future revision of this policy as Appendix C.

All WVI/FC information will be periodically reviewed for relevancy and importance. Information which has been determined to be invalid, untrue, obsolete, no longer useful because the purpose for which it was collected has been satisfied or no longer exists will be purged, destroyed, and deleted from the system. The WVI/FC is not required by law or regulation to notify, and will not notify source agencies of the purge of information or intelligence from WVI/FC databases unless otherwise provided in source agency participation agreements. Source agencies will not be notified when information they have submitted is due for purge from WVI/FC information or intelligence databases. Purge dates will be tracked in electronic databases based on the date of record entry into the database.

## N. Accountability and Enforcement

### N.1 Information System Transparency

The WVI/FC will be open with the public in regard to information and intelligence collection practices. The WVI/FC's Privacy Policy will be provided to the public upon request and will also be posted on the WVI/FC Web site at Fusioncenter.wv.gov as well as on the National Fusion Center Web site once it is established.

The WVI/FC's Privacy Officer will be responsible for receiving inquiries and complaints about privacy, civil rights, and civil liberties protections in WVI/FC information system(s). The WVI/FC's Privacy Officer will report all inquiries and complaints to the Director.

### N.2 Accountability

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

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

The WVI/FC's Privacy Officer will randomly and annually conduct audits to ensure and evaluate the compliance of users. A record of the audits will be maintained by the Privacy Officer.

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

The Privacy Officer will conduct both randomly and annually audits and inspections of the WVI/FC's Watch Center's information. 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).

The WVI/FC's Oversight Committee, guided by the trained Privacy Officer, will review and recommend updates to this policy to the Director at least annually in response to changes in applicable law, technology, the purpose and use of the information systems, public expectations, and experience in policy implementation.

**N.3 Enforcement**

If an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification or disclosure of information, the Director of the WVI/FC will, if necessary, refer the matter to appropriate authorities for criminal prosecution, or:

- Notify in writing the chief executive of the employing agency of the violation and noncompliance of his or her employee and initiate an investigation, if appropriate.

- As the WVI/FC is a multi-agency effort, WVI/FC's Director will work with each agency regarding their personnel policies for appropriate sanctions for noncompliance that does not rise to the level of a criminal matter.

- Agencies must take action to correct such violations and provide an assurance in writing to the WVI/FC Director that corrective action has been taken.

- The failure to remedy violations may result in suspension or termination of access by the employee to WVI/FC information.

- The WVI/FC reserves the right to restrict the qualifications and number of personnel having direct access to WVI/FC information, and to suspend or withhold service to any participating agency user who fails to comply with the applicable restrictions and limitations of the WVI/FC's Privacy Policy.

**O. Training**

The WVI/FC will require annual training for any person who is granted direct access to WVI/FC information regarding implementation of and adherence to the Privacy Policy.

The WVI/FC will also provide training to personnel authorized to share protected information through the ISE.

The WVI/FC'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 WVI/FC;

• Originating and participating agency responsibilities and obligations under applicable law and policy.

• How to implement the policy in the day-to-day work of the user, whether a paper or systems user;

• The impact of improper activities associated with infractions within or through the agency;

• Mechanisms for reporting violations of WVI/FC privacy-protection policies; and

• The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

## Appendix A – Definitions

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

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

**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.

**Agency –** Agency refers to all agencies that access, contribute, and share information in the information system.

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

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

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

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

**Authorized User –** A person that is granted direct access to WVI/FC 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. The latter includes voiceprints and handwritten signatures.

**Call Log Information Sheet –** The input form used by WVI/FC personnel in the WVI/FC Watch Center to record information received and disseminated. The information maintained on

the Call Log Information Sheet will be sufficient to identify the individual making the request, accessing information, or receiving disseminated information from WVI/FC as well as the nature of the information.

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

**Civil Liberties –** Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of 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.

**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 –** Inserts, symbols, signs, descriptions, or measures.

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

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

**Electronically 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.

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

Collection Limitation Principle
Data Quality Principle
Purpose Specification Principle
Use Limitation Principle
Security Safeguards Principle
Openness Principle
Individual Participation Principle
Accountability Principle

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

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

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

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

**Individual Responsibility –** 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; 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 –** 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 – 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 –** 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 are getting access to the data. (See also Audit Trail.)

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

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

**Need to Know—** As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

**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.

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

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

**Personally Identifiable Information –** Personally identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:
• Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
• A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
• Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
• Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc).

**Persons –** Executive Order 12333 defines "United States persons" as 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 –** Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy

include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

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

**Privacy Protection –** This is a process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

**Private Records** – A private record is a record that identifies, or can be used to identify, locate, contact, or impersonate an individual. Additionally, the record contains information, which if it were disclosed, could jeopardize private or protected information.

**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 West Virginia constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; and applicable state, local, and tribal laws and ordinances. Protection may also be extended to organizations by center policy or state, local, or tribal 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 –** Internal procedures to address complaints from persons regarding protected information about them that is under the agency's/center's control.

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

**Retention –** (Refer to Storage.)

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

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

**Role-Based 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.

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

**Storage –** In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:
Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry.

In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.
With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information—including homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland—by both the originator of the information and any recipient of the information.

With regard to the WVI/FC, storage (or retention) refers to the storage and safeguarding of, among other things, 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—**Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

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

**Terrorism Information—**Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

**Terrorism-Related Information—**In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. §

482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include intelligence information.
Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

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

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

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

**WVI/FC Watch Center –** The location within the West Virginia Intelligence/Fusion Center where information is received, assessed, disseminated and retained.

## 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

**ATTENTION: This Privacy Policy is a working and living document, to be molded by both law and settled cases. It will be continuously updated and revised to reflect the current laws and cases so as to ensure both the rights and the security of the people. Make sure that you contact the West Virginia Intelligence/Fusion Center for the most recent and accurate version.**