

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Vincent C. Gray
Mayor



Chris T. Geldart
Director

MEMORANDUM

DATE: April 21, 2014
TO: Washington Regional Threat Analysis Center (WRTAC)
FROM: Chris Geldart, Director *CG*
RE: HSEMA Policy: Washington Regional Threat Analysis Center Privacy Policy
Policy No. 2014-702

Effective today, this memorandum implements Policy No. 2014-702, Washington Regional Threat Analysis Center Privacy Policy (attached hereto). The purpose of this privacy, civil rights, and civil liberties protection policy is to promote Washington Regional Threat Analysis Center and user conduct that complies with applicable federal, state, local, and tribal law and assists the center and its users in:

- A. Increasing public safety and improving national security;
- B. Minimizing the threat and risk of injury to specific individuals;
- C. Minimizing the threat and risk of physical or financial injury to law enforcement, first responders and others responsible for public protection, safety, or health;
- D. Minimizing the threat and risk of damage to real or personal property;
- E. Protecting individual privacy, civil rights, civil liberties, and other protected interests;
- F. Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;
- G. Minimizing reluctance of individuals or groups to use or cooperate with the justice system;
- H. Supporting the role of the justice system in society;
- I. Promoting governmental legitimacy and accountability;
- J. Not unduly burdening the ongoing business of the justice system; and
- K. Making the most effective use of public resources allocated to public safety agencies.

Questions regarding the purpose or application of any section of this policy should be referred to me at 202-727-6161 or Tip Wight, WRTAC Executive Director, at 202-481-3087 or lee.wight@dc.gov.

Washington Regional Threat Analysis Center Interim Privacy Policy

TABLE OF CONTENTS

I. PURPOSE STATEMENT 2

II. POLICY APPLICABILITY AND LEGALITY COMPLIANCE 2

III. GOVERNANCE AND OVERSIGHT 3

IV. DEFINITIONS 4

V. INFORMATION 4

VI. ACQUIRING AND RECEIVING INFORMATION 7

VII. INFORMATION QUALITY ASSURANCE 8

VIII. COLLATION AND ANALYSIS 9

IX. MERGING RECORDS 10

X. SHARING AND DISCLOSURE 10

XI. REDRESS 12

XII. SECURITY SAFEGUARDS 13

XIII. INFORMATION RETENTION AND DESTRUCTION 14

XIV. ACCOUNTABILITY AND ENFORCEMENT 15

XV. TRAINING 16

XVI. APPENDICES 18

A. Terms and Definitions 18

B. Federal and District of Columbia Statutes 27

I. GENERAL/BACKGROUND

The Washington Regional Threat Analysis Center, or WRTAC, is the designated fusion center for the District of Columbia and also serves the National Capital Region (NCR). Its mission statement is: to facilitate the full integration of available data in the region to detect, prevent, and respond to terrorist and other criminal activity, as well as facilitate information sharing during any catastrophic event in the NCR.

II. PURPOSE STATEMENT

The purpose of this privacy, civil rights, and civil liberties protection policy (Policy) is to promote Washington Regional Threat Analysis Center (WRTAC or Center) and user conduct that complies with applicable federal, state, local, and tribal law (*see* Section XVIII, Appendix B, “Federal and District of Columbia Statutes”) and assists the center and its users in:

- A. Increasing public safety and improving national security;
- B. Minimizing the threat and risk of injury to specific individuals;
- C. Minimizing the threat and risk of physical or financial injury to law enforcement, first responders and others responsible for public protection, safety, or health;
- D. Minimizing the threat and risk of damage to real or personal property;
- E. Protecting individual privacy, civil rights, civil liberties, and other protected interests;
- F. Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;
- G. Minimizing reluctance of individuals or groups to use or cooperate with the justice system;
- H. Supporting the role of the justice system in society;
- I. Promoting governmental legitimacy and accountability;
- J. Not unduly burdening the ongoing business of the justice system; and
- K. Making the most effective use of public resources allocated to public safety agencies.

III. ROLES AND RESPONSIBILITIES

- A. The Privacy Officer is the point of contact for reporting alleged errors and violations of privacy policy and ensures that privacy protections are implemented and maintained through training, policy changes and audits.
- B. The Administrative Support Staff is responsible for all WRTAC administrative and logistical matters. The Administrative Support Staff will document all training of staff conducted under this policy.

IV. POLICY APPLICABILITY AND LEGALITY COMPLIANCE

- A. The Executive Director, Privacy Officer, HSEMA/WRTAC personnel, interns, liaisons, and participating District of Columbia agencies or other personnel, anyone providing information technology services to WRTAC, private contractors, and other authorized users will comply with the Center’s privacy policy and applicable law protecting privacy,

civil rights, and civil liberties, including, but not limited to those cited in Section XVIII, Appendix B “Federal and District of Columbia Statutes” of this Policy.

- B.** This Policy applies to information the WRTAC gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to Center personnel, governmental agencies (including Information Sharing Environment (ISE) participating centers and agencies), and, participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.
- C.** The WRTAC will provide a printed or electronic copy of this policy to all Center and non-Center personnel who provide services and to participating agencies and individual users and will require both a written acknowledgement of receipt of this Policy and a written agreement to comply with this Policy and the applicable provisions it contains.
- D.** The WRTAC has adopted internal operating policies that are in compliance with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. Constitution and the First Amendment Assemblies Act of 2004, D.C. Code §§5-331.01 to 5-331.17.

NOTE: With the exception of the Executive Director, who is an employee of the Metropolitan Police Department detailed to HSEMA and the Privacy Officer, who is an employee of the Office of the Attorney General, all other WRTAC staff are District of Columbia Homeland Security and Emergency Management Agency (“HSEMA”) personnel.

V. GOVERNANCE AND OVERSIGHT

- A.** Mayor’s Order 2012-37 designated HSEMA as the “primary fusion center for the District of Columbia.” The Administrative control and the day to day operations of the WRTAC are the responsibility of HSEMA.
- B.** Responsibility for the operation of the WRTAC; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this Policy is assigned to the Executive Director of the Center.
- C.** The WRTAC receives advice and guidance from the District of Columbia Fusion Center Advisory Board (Mayor’s Order 2012-204). The Board’s purpose is to “develop a proposed operational framework for the WRTAC” which would include “policies that are designed to ensure that individuals’ constitutional rights, civil liberties, civil rights and privacy interests are protected at all times.” HSEMA and WRTAC will submit substantive policies to the Advisory Board for review and comment.
- D.** The WRTAC is guided by a trained Privacy Officer who is appointed by the Director of HSEMA. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this Policy, receives and coordinates complaint resolution, and serves as the liaison for the Information Sharing Environment. The Privacy Officer can be contacted at the following address, WRTAC@dc.gov, Attention: Privacy Officer. The WRTAC’s Privacy Officer ensures that enforcement procedures and sanctions outlined in Section XIV(C), “Enforcement,” are adequate and enforced. The Privacy Officer will annually review and update the policy in response to changes in law and implementation experience, including the results of audits and inspections.

VI. DEFINITIONS

See Section XVIII, Appendix A, “Terms and Definitions” for a listing of the terms and definitions used in this Policy.

VII. INFORMATION

- A.** The WRTAC will seek or retain information that:
1. Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents, threats to critical infrastructure and/or that which might occasion a fire, emergency management, or public health response; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
 2. Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
 3. The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
 4. The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.
- B.** WRTAC may retain protected information that is based on a level of suspicion that is less than “reasonable suspicion,” such as tips and leads or Suspicious Activity Report (SAR) information, subject to the policies and procedures specified in this Policy. The WRTAC 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 races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations. Retained information will be reviewed annually to ensure that retained information is still relevant and required for retention in accordance with the provisions of the Criminal Intelligence Systems Operating Policies, 28 C.F.R. §§ 23.1-23.40 (2012) and the procedures prescribed within this Policy.
- C.** WRTAC staff and any participating agencies will not violate the Electronic Communications Privacy Act of 1986, Pub. Law No. 99-508, 18 U.S.C. §§ 2510–2520, 2701–2709, and 3121–3125 or any other applicable District of Columbia statute related to wiretapping and surveillance.
- D.** The WRTAC applies labels to WRTAC-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:
1. The information is protected information as defined by the Center, to include personal information on any individual (*see* Center’s definitions of “protected information” and “personal information” in Section XVIII, Appendix A “Terms and Definitions” of Policy), and, to the extent expressly provided in this Policy, to include organizational entities.
 2. The information is subject to District of Columbia and federal law restricting access, use, or disclosure. *See* U.S. CONST. amend. I; D.C. Code §5-331.03, First Amendment Rights and Police Standards; and D.C. Official Code §§5-331.01-

337.01; 2-534; 2-1707; 4-1305.08; 5-113.06; 7-1201.02; 7-1605; 14-307; 16-2331-2336.

- E.** The WRTAC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:
1. Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
 2. The nature of the source as it affects veracity (*i.e.*, anonymous tip, trained interviewer or investigator, public record, private sector).
 3. The reliability of the source (*i.e.*, reliable, usually reliable, unreliable, unknown).
 4. The validity of the content (*i.e.*, confirmed, probable, doubtful, cannot be judged).
- F.** At the time a decision is made by the WRTAC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:
1. Protect confidential sources and police undercover techniques and methods.
 2. Not interfere with or compromise pending criminal investigations.
 3. Protect an individual's right of privacy or their civil rights and civil liberties.
 4. Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.
- G.** The labels assigned to existing information under Section VI, "Information," at (F) will be reevaluated whenever:
1. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
 2. 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.
- H.** WRTAC 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:
1. 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 follow its SAR policy which includes a standard reporting format and data collection guidelines for SAR information.
 2. Store the information using the same storage method used for data that 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.

3. 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 (*i.e.*, “need-to-know” and “right-to-know” access or dissemination for personally identifiable information).
 4. 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.
 5. Retain an invalidated tip, lead, or SAR information long enough 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.
 6. Adhere to and follow the WRTAC’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.
- I.** The WRTAC 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.
- J.** The WRTAC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.
- K.** The WRTAC 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:
1. The name of the originating center, department or agency, component, and subcomponent.
 2. The name of the center’s justice information system from which the information is disseminated.
 3. The date the information was collected and, where feasible, the date its accuracy was last verified.
 4. The title and contact information for the person to whom questions regarding the information should be directed.
- L.** The WRTAC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or

disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

- M. The WRTAC will keep a record of the source of all information sought and collected by the center.

VIII. ACQUIRING AND RECEIVING INFORMATION

- A. Information-gathering (acquisition) and access and investigative techniques used by the WRTAC and information-originating agencies will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:
1. Criminal Intelligence Systems Operating Policies 28 C.F.R. §§ 23.1-23.40 (2012).
 2. The Organization for Economic Co-operation and Development (OECD) Fair Information Principles:
 - a. Collection Limitation Principle
 - b. Data Quality Principle
 - c. Purpose Specification Principle
 - d. Use Limitation Principle
 - e. Security Safeguards Principle
 - f. Openness Principle
 - g. Individual Participation Principle
 - h. Accountability Principle

(Note: Under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the Federal Privacy Act; state, local, and tribal law; or WRTAC policy). See OECD Privacy Principles, <http://oecdprivacy.org/>.
 3. Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ), *National Criminal Intelligence Sharing Plan* (NCISP) (2003) http://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf.
 4. Constitutional provisions (*i.e.*, First Amendment) and other federal and District laws cited in the appendices. See Section XVIII, Appendix B, "Federal and District of Columbia Statutes."
- B. The WRTAC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating HSEMA staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.
- C. The WRTAC'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.

- D. Information-gathering and investigative techniques used by the WRTAC 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.
- E. External agencies that receive WRTAC information or share information with the Center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.
- F. WRTAC will restrict the dissemination of criminal intelligence information to those law enforcement authorities who agree to follow procedures regarding information receipt, maintenance, security, and dissemination that are consistent with the Criminal Intelligence Systems Operating Policies 28 C.F.R. §§ 23.1-23.40 (2012) operating principles (except that an assessment of criminal or other information may be disseminated when necessary to avoid imminent danger to life or property).
- G. The WRTAC 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.
- H. The WRTAC will not directly or indirectly receive, seek, accept, or retain information from:
 - 1. An individual or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or WRTAC policy.
 - 2. An individual or information provider that is legally prohibited from obtaining or disclosing the information.

IX. INFORMATION QUALITY ASSURANCE

- A. The WRTAC 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 (*see* Section XI, Merging Records) has been met.
- B. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence (verifiability and reliability)).
- C. The WRTAC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.
- D. The labeling of retained information will be reevaluated by the WRTAC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.
- E. The WRTAC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the Center did not have authority to gather the information or to provide the information to another agency; or the WRTAC used

prohibited means to gather the information (except when the Center's information source did not act as the agent of the Center in gathering the information).

- F.** Originating agencies external to the WRTAC are responsible for reviewing the quality and accuracy of the data provided to the Center. The Center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable before further dissemination or using that information in WRTAC analyses.
- G.** The WRTAC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

X. COLLATION AND ANALYSIS

- A.** Information acquired or received by the WRTAC 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.
- B.** Information subject to collation and analysis is information as defined and identified in Section VII, "Information," or other appropriate Policy section.
- C.** Information acquired or received by the WRTAC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:
 - 1. Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.
 - 2. 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 (including terrorist) activities.
 - 3. Further emergency management efforts, including fire, public health and other emergent situations that threaten the life, property, and public safety of the citizens of the District of Columbia and its associated City agencies and public or private non-governmental organizations within the City as specified by the WRTAC Advisory Board
 - 4. Protect and mitigate all-source threats against District of Columbia critical infrastructure as designated by the City
- D.** The WRTAC requires that all organically produced analytical products containing any privacy act protected information on US persons be reviewed and approved before dissemination 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.
- E.** Additionally, all WRTAC employees, interns and liaison officers involved in the production, review, or dissemination will complete Criminal Intelligence Systems Operating Policies 28 C.F.R. §§ 23.1-23.40 (2012) training annually and the WRTAC Executive Assistant will maintain documentation of that training. Additionally, the WRTAC Privacy Officer will conduct periodic and random reviews of WRTAC products

to ensure they are in compliance with these policies, in addition to any external inspection or peer reviews mandated or conducted by or in partnership with DHS. The results of all inspections will be maintained by WRTAC for a period of not less than 10 years.

XI. MERGING RECORDS

- A.** The set of identifying information sufficient to allow merging by the WRTAC 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.
- B.** If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the WRTAC if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

XII. SHARING AND DISCLOSURE

- A.** Credentialed, role-based access criteria will be used by the WRTAC, as appropriate, to control:
 - 1. The information to which a particular group or class of users can have access based on the group or class.
 - 2. The information a class of users can add, change, delete, or print.
 - 3. To whom, individually, the information can be disclosed and under what circumstances.
- B.** The WRTAC 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.
- C.** Access to or disclosure of records retained by the WRTAC will be provided only *to persons within the Center 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. An audit trail sufficient to allow the identification of each individual who accessed information retained by WRTAC and the nature of the information accessed will be kept by the Center.
- D.** Agencies external to the WRTAC may not disseminate information covered within this document or under the Criminal Intelligence Systems Operating Policies 28 C.F.R. §§

23.1-23.40 (2012) that is accessed by or disseminated from the center without approval from the Center or other originator of the information.

- E. Records retained by the WRTAC may be accessed by or disseminated *to those responsible for public protection, public safety, or public health* only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.
- F. Information gathered or collected and records retained by the WRTAC 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 5 years by WRTAC.
- G. Information gathered or collected and records retained by the WRTAC 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 WRTAC 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.
- H. Information gathered or collected and records retained by the WRTAC ***will not be***:
 - 1. Sold, published, exchanged, or disclosed for commercial purposes.
 - 2. Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
 - 3. Disseminated to persons not authorized to access or use the information.
- I. There are several categories of records that will ordinarily *not be provided* to the public:
 - 1. Information exempt from disclosure under D.C. Code § 2-534 (2013).
 - 2. Information that meets the definition of "classified information" as that term is defined in the National Security Act of 1947, Pub. L. No. 235-606 (2007).
 - 3. Information exempt from disclosure pursuant to D.C. Code § 2-1707 (2013).
 - 4. Information exempt from disclosure pursuant to D.C. Code § 4-1305.08 (2013).
 - 5. Information exempt from disclosure pursuant to D.C. Code § 5-113.06 (2013).
 - 6. Information exempt from disclosure pursuant to D.C. Code § 7-1605 (2013).
 - 7. Information exempt from disclosure pursuant to D.C. Code § 14-307 (2013).
 - 8. Information exempt from disclosure pursuant to D.C. Code §§ 16-2331 to 16-2336 (2013).
 - 9. Information exempt from disclosure pursuant to D.C. Code § 16-2394 (2013).
 - 10. Information of personally identifiable health information pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 or any other confidentiality law.

11. Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission.
 12. A violation of an authorized nondisclosure agreement.
- J.** The WRTAC 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.

XIII. REDRESS

A. Disclosure

1. Upon 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 WRTAC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The WRTAC's response to the request for information will be made within the time frame mandated by the District of Columbia Freedom of Information Act, DC Code § 2-531, et seq. A record will be kept of all requests and of what information is disclosed to an individual.
2. The existence, content, and source of the information will not be made available by the WRTAC to an individual when the information is exempt from disclosure pursuant to D.C. Code §2-534 (2013) and Section XII (I), "Sharing and Disclosure" and:
 - a. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
 - b. Disclosure would endanger the health or safety of an individual, organization, or community;
 - c. The information is in a criminal intelligence information system subject to Criminal Intelligence Systems Operating Policies 28 C.F.R. §§ 23.1-23.40 (2012).
 - d. The information is exempt from disclosure pursuant to the provisions in Section XII (I), "Sharing and Disclosure" and Section VII (C), "Information."
 - e. The information source does not reside with the center.
 - f. The center did not originate and does not have a right to disclose the information.
 - g. Other *authorized* basis for denial.
3. If the information does not originate with the WRTAC, the requestor will be referred to the originating agency, if appropriate or required, 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.

B. Corrections

If an individual requests correction of information originating with the WRTAC that has been disclosed, they will be referred to the WRTAC Privacy Officer. A record will be kept of all requests for corrections and the resulting action, if any.

C. Appeals

The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the WRTAC or the originating agency. The individual will also be informed of the procedure for appeal when the center or originating agency 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. *See* D.C. Code § 2-537 (2013).

D. Complaints

1. 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;
 - c. Is held by the WRTAC; and
 - d. Allegedly has resulted in demonstrable harm to the complainant; then
2. WRTAC 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 the following address: WRTAC@dc.gov, Attention: 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.
3. If the information did not originate with WRTAC, 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.
4. All information held by the center 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, WRTAC will not share the information until such time as the complaint has been resolved. A record will be kept by the Center of all complaints and the resulting action taken in response to the complaint.
5. To delineate protected information shared through the ISE from other data, the WRTAC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

XIV. SECURITY SAFEGUARDS

- A.** The WRTAC has designated and trained an HSEMA staff member to serve as the Center's security officer.

- B. The WRTAC will operate in a secure facility protected from external intrusion. The Center will utilize secure internal and external safeguards against network intrusions. Access to WRTAC's databases from outside the facility will be allowed only over secure networks.
- C. The WRTAC 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 the Criminal Intelligence Systems Operating Policies, 28 C.F.R. §§ 23.1-23.40 (2012).
- D. The WRTAC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
- E. Access to WRTAC 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.
- F. The WRTAC will utilize watch logs to maintain audit trails of requested and disseminated information.
- G. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.
- H. The WRTAC will follow the data breach notification guidance set forth in Office of Management and Budget, Memorandum M-07-16, <http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf> (May 2007).
- I. The WRTAC will immediately notify the originating agency from which the Center received personal information of a suspected or confirmed breach of such information.

XV. INFORMATION RETENTION AND DESTRUCTION

- A. All applicable information will be reviewed for record retention (validation or purge) by WRTAC at least every five (5) years, as provided by the Criminal Intelligence Systems Operating Policies, 28 C.F.R. §§ 23.1-23.40 (2012).
- B. When information has no further value or meets the criteria for removal according to the WRTAC's retention and destruction Policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.
- C. The WRTAC will delete information or return it to the originating agency once its retention period has expired as provided by this Policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.
- D. No approval will be required from the originating agency before information held by the WRTAC is destroyed or returned in accordance with this Policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.
- E. Notification of proposed destruction or return of records may or may not be provided to the originating agency by the WRTAC, depending on the relevance of the information and any agreement with the originating agency.
- F. A record of information to be reviewed for retention will be maintained by the WRTAC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

XVI. ACCOUNTABILITY AND ENFORCEMENT

A. Information System Transparency

1. The WRTAC will be open with the public in regard to information and intelligence collection practices. WRTAC's Privacy Policy will be provided to the public for review upon request, and posted on any websites maintained by HSEMA. Currently, the WRTAC Privacy Policy is located on HSEMA's Freedom of Information Act (FOIA) website: <http://hsema.dc.gov/page/hsema-foia-requests>.
2. The WRTAC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Officer can be contacted at the following address: WRTAC@dc.gov, Attention: Privacy Officer.

B. Accountability

1. The audit log of queries made to the WRTAC will identify the user initiating the query.
2. The WRTAC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.
3. The WRTAC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this Policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. Audits will occur at least semiannually and a record of the audits will be maintained by the Privacy Officer of the Center.
4. The WRTAC's personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the Center's Privacy Officer. *See* Section V, "Governance and Oversight."
5. The WRTAC will conduct an audit and inspection of the information and intelligence contained in its information system(s) on a quarterly basis. The audit will be conducted by a designated independent panel. This independent panel has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of WRTAC. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the Center's information and intelligence system(s).
6. The WRTAC's Advisory Board, guided by the appointed and trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy **annually** and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

C. Enforcement

1. If Center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this Policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of the WRTAC will:
 - a. Suspend or discontinue access to information by the Center personnel, the participating agency, or the authorized user.
 - b. Suspend, reprimand, transfer, or terminate Center personnel, as permitted by applicable personnel policies.
 - c. Apply administrative actions or sanctions as provided by D.C. Code § 2-537 (2013); D.C. Code §§16-2336, 16-2394 (2013); “Disciplinary Procedures and Processes,” General Order 120.21 (2006); and other pertinent regulations as provided in agency and center personnel policies.
 - d. If the authorized user is from an agency external to the WRTAC, the Director will request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy’s provisions.
 - e. Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy
2. The WRTAC reserves the right to restrict the qualifications and number of personnel having access to Center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the Center’s Privacy Policy.

XVII. TRAINING

- A. The WRTAC will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties Policy:
 1. All WRTAC assigned personnel, including interns and liaison officers (LNOs).
 2. Personnel providing information technology services to the Center.
 3. Staff in other public agencies or private contractors providing services to the center.
 4. Users who are not employed by the Center or contractors.
 5. Any person who physically transits the center spaces on a recurring basis or physically works closely with WRTAC personnel inside the WRTAC spaces, such as HSEMA personnel who would likely come into contact with privacy act information based on the nature of their duties and association with WRTAC personnel and systems.
 6. In addition to the below training, all applicable personnel above will also complete the on-line 28 C.F.R. §§ 23.1-23.40 (2012) training on a frequency specified within the parent directives. The WRTAC Administrative Assistant will maintain a record of this training.
- B. The WRTAC will provide special training regarding the Center’s requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

- C. The WRTAC's privacy policy training program will cover:
1. Purposes of the privacy, civil rights, and civil liberties protection policy.
 2. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the center.
 3. Originating and participating agency responsibilities and obligations under applicable law and policy.
 4. How to implement the policy in the day-to-day work of the user, whether a paper or systems user.
 5. The impact of improper activities associated with infractions within or through the agency.
 6. Mechanisms for reporting violations of center privacy protection policies and procedures.
 7. The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

XVIII. APPENDICES

A. Terms and Definitions

The following is a list of primary terms and definitions used throughout this policy.

1. *Access* - Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access. With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.
2. *Acquisition* - The means by which an ISE participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.
3. *Audit Trail* - A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.
4. *Authentication* - The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. *See* Biometrics, 7, below.
5. *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.
6. *Center* - Refers to the WRTAC and all participating state agencies of the WRTAC.
7. *Civil Liberties* - Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Generally, the term “civil rights” involves positive (or affirmative) government action, while the term “civil liberties” involves restrictions on government.

8. *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.
9. *Confidentiality* - Closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. *See Privacy.*
10. *Criminal Intelligence Information* - Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 C.F.R. §§ 23.1-23.40 (2012).
11. *Data* - Inert symbols, signs, descriptions, or measures; elements of information.
12. *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.
13. *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.
14. *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:

- a. Collection Limitation Principle
- b. Data Quality Principle
- c. Purpose Specification Principle
- d. Use Limitation Principle
- e. Security Safeguards Principle
- f. Openness Principle
- g. Individual Participation Principle
- h. Accountability Principle•

15. *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.
16. *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.
17. *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.
18. *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, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information.
19. *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.

20. *Information Sharing Environment (ISE) Suspicious Activity Report (SAR)* (Collectively “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).
21. *Invasion of Privacy* - Intrusion on one’s solitude or into one’s private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one’s name or picture for personal or commercial advantage. *See also* Right to Privacy.
22. *Law* - As used by this policy, law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.
23. *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.
24. *Lawful Permanent Resident* - A foreign national who has been granted the privilege of permanently living and working in the United States.
25. *Logs* - A necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the data. *See also* Audit Trail.
26. *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.
27. *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.

28. *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.
29. *Participating Agency* - An organizational entity that is authorized to receive and use center information for lawful purposes.
30. *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.
31. *Personally Identifiable Information* - One or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:
 - a. 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).
 - b. 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).
 - c. Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
 - d. Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).
32. *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.
33. *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.
34. *Privacy Policy* - A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information

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

35. *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.
36. *Protected Information* - For the non-intelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. While not within the definition established by the ISE Privacy Guidelines, protection may be extended to other individuals and organizations by internal federal agency policy or regulation. For the (federal) intelligence community, protected information includes information about “United States persons” as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered. For state, local, and tribal governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 C.F.R. §§ 23.1-23.40 (2012); applicable state and tribal constitutions; and applicable state, local, and tribal laws, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion center or other state, local, or tribal agency policy or regulation.
37. *Public* –
 - a. Public includes:
 - i. Any person and any for-profit or nonprofit entity, • organization, or association.
 - ii. Any governmental entity for which there is no • existing specific law authorizing access to the center’s information.
 - iii. Media organizations.
 - iv. Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the center or participating agency.
 - b. Public does not include:
 - i. Employees of the center or participating agency.
 - ii. People or entities, private or governmental, who assist the center in the operation of the justice information system.
 - iii. Public agencies whose authority to access • information gathered and retained by the center is specified in law.

38. *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.
39. *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.
40. *Redress* - Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the center's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.
41. *Retention* - Refer to Storage.
42. *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.
43. *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.
44. *Role-Based Access* - A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.
45. *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.
46. *Source Agency* - Source agency refers to the agency or organizational entity that originates SAR (and when authorized, ISE-SAR) information.
47. *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:
 - a. 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.
 - b. In a more formal usage, storage has been divided into:
 - i. 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
 - ii. Secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.
 - iii. 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.

- c. 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.
48. *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.
 49. *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.
 50. *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.
 51. *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.

52. *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.
53. *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.

B. Federal and District of Columbia Statutes

Following is a partial listing of applicable federal and District of Columbia laws:

1. FEDERAL LAW

- a. Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A (2013).
- b. Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a); Office of Management and Budget, Memorandum M-01-05, Guidance on Interagency Sharing of Personal Data—Protecting Personal Privacy (2000).
- c. Confidentiality of Identifiable Research and Statistical Information, 28 C.F.R §§22.1-22.29 (1999).
- d. Crime Identification Technology, 42 U.S.C. § 14601 (2013).
- e. Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611 (2013).
- f. Criminal Intelligence Systems Operating Policies, 28 C.F.R. §§ 23.1-23.40 (2012).
- g. Disposal of Consumer Report Information and Records, 16 C.F.R. §§ 682.1-682.5 (2004).
- h. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, 3121-3125 (2013).
- i. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2013).
- j. Federal Civil Rights Laws, 42 U.S.C. § 1983 (2013).
- k. Federal Records Act, 44 U.S.C. § 3301 (2013).
- l. Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2013).
- m. HIPAA, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996).
- n. HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160, 164 (2013).
- o. Indian Civil Rights Act of 1968, 25 U.S.C. § 1301 (2013).
- p. Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458 (2004).
- q. National Child Protection Act of 1993, Pub. L. No. 103-209 (1993).
- r. National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616 (2013).
- s. Privacy Act of 1974, 5 U.S.C. § 552a (2013).
- t. Privacy of Consumer Financial Information, 16 C.F.R. §§ 313.1-313.18 (2013).
- u. Protection of Human Subjects, 28 C.F.R. §§ 46.101-46.124 (2013).
- v. Standards for Safeguarding Customer Information, 16 C.F.R. §§ 314.1-314.5 (2013).
- w. Sarbanes-Oxley Act of 2002, 15 U.S.C. §§ 7201-7266 (2013).
- x. U.S. CONST. amends. I, IV, and VI.
- y. USA PATRIOT Act, Pub. L. No. 107-56 (2001).

2. DISTRICT OF COLUMBIA LAW

- a. First Amendment Assemblies Act of 2004, D.C. Code §§ 5-331.01 to 5-337.01 (2013).
- b. D.C. Code § 1-615.51 (2013).
- c. D.C. Code § 2-1707 (2013).
- d. D.C. Code §§ 2-531 to 2-537 (2013).
- e. D.C. Code § 2-5417 (2013).
- f. D.C. Code § 4-1305.08 (2013).
- g. D.C. Code § 5-113.06 (2013).
- h. D.C. Code § 5-417 (2013).
- i. D.C. Code § 7-1201.02 (2013).
- j. D.C. Code § 7-1605 (2013).
- k. D.C. Code § 7-2301 (2013).
- l. D.C. Code § 7-2271 (2013).
- m. D.C. Code § 14-307 (2013).
- n. D.C. Code § 16-2331 to 16-2336 (2013).
- o. D.C. Code § 16-2393 to 16-2394 (2013).
- p. D.C. Code § 22-3152 (2013).
- q. D.C. Code § 28-4505 (2013).
- r. D.C. Code § 44-801 (2013).
- s. D.C. Code § 47-2851.06 (2013).
- t. General Order 120.21 (2013).