National Capital Region Threat Intelligence Consortium

2720 Martin Luther King, Jr. Avenue
Washington, DC 20032
NTIC@dc.gov
202-481-3075 (office)

Privacy Policy

DECEMBER 2018

National Capital Region Threat Intelligence Consortium
Privacy Policy

Table of Contents

A. Purpose Statement

The purpose of this privacy, civil rights, and civil liberties protection policy is to promote National Capital Region Threat Intelligence Consortium (NTIC) and user conduct that complies with applicable federal, state, local, and tribal law (see Appendix A, Terms and Definitions) and assists the center and its 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 physical or financial 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 the criminal investigatory, 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.
- Making the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legality Compliance

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

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

3. All NTIC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center

information originates, and other authorized users will comply with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to [those Federal and D.C. statutes cited in the appendices to this policy.]

4. The NTIC has adopted internal operating policies that comply 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. *See* D.C. Official Code §§ 5-331.01-337.01.

C. Governance and Oversight

1. Primary responsibility for the operation of the NTIC; 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 Director of the center.

2. The NTIC is guided by an Executive Board of Directors that liaises with the community to ensure that privacy and civil rights are protected as provided in this policy and by the center's information gathering and collection, retention, and dissemination processes and procedures. The 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.

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

4. The NTIC's Privacy Officer ensures that enforcement procedures and sanctions outlined in (see Section N.3, Enforcement) are adequate and enforced.

D. Definitions

1. For primary terms and definitions used in this Policy, refer to Appendix A, Terms and Definitions.

E. Information

1. The NTIC will seek or retain information that:

   - Is based on a possible threat to public safety or the enforcement of the criminal law, 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, or 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.

   The center 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.

2. The NTIC will not seek or retain, and information originating agencies will agree not to submit information about individuals or organizations solely based on 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.

3. The NTIC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to authorized consumers user that:

   - The information is protected personal information (*see* center's definitions of "protected information" and

"personal information" in Appendix A of policy), and, to the extent expressly provided in this policy, to include organizational entities.
- The information is subject to D.C. and federal law restricting access, use, or disclosure. [U.S. Constitution; the First Amendment Assemblies Act of 2004. *See* D.C. Official Code §§ 5-331.01-337.01; and D.C. Official Code §§ 2-534; 2-1707; 4-1305.08; 5-113.06; 7-1201.02; 7-1605; 14-307; 16-2331-2336.]

4. The NTIC 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:

    - 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.
    - The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
    - The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
    - The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. At the time a decision is made by the NTIC 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:

    - Protect confidential sources and police undercover techniques and methods.
    - Not interfere with or compromise pending criminal investigations.
    - Protect an individual's right of privacy or their civil rights and civil liberties.
    - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The labels assigned to existing information under (see Section E.5 above) will be reevaluated whenever:

    - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
    - There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7. NTIC 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 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.
    - 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 an invalidated tip, lead, or SAR information for five years 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.

8. The NTIC 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.

9. The NTIC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information

Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The NTIC 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.

11. The NTIC 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.

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

F. Acquiring and Receiving Information

1. Information-gathering (acquisition) and access and investigative techniques used by the NTIC 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 (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 center policy).
    - Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).

- Constitutional provisions, *i.e.*, First Amendment; District laws cited in the appendices of this policy**;** and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

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

3. The NTIC'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.

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

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

6. The NTIC 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.

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

G. Information Quality Assurance

1. The NTIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard [refer to Section I, Merging Records,] has been met.

2. 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]).

3. The NTIC 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.

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

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

6. Originating agencies external to the NTIC 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.

7. The NTIC 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.

H. Collation and Analysis

1. Information acquired or received by the NTIC 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.

2. Information subject to collation and analysis is information as defined and identified in [Refer to Section E, Information, or appropriate policy section]

3. Information acquired or received by the NTIC 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, public safety, force deployment, or prosecution objectives and priorities established by the center.
   - 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.

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

I. Merging Records

1. The set of identifying information sufficient to allow merging by the NTIC 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.

2. If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the NTIC 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

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

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

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

3. Access to or disclosure of records retained by the NTIC 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, 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 the center and the nature of the information accessed will be kept by the center.

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

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

6. Information gathered or collected, and records retained by the NTIC 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 the center.

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

8. Information gathered or collected, and records retained by the NTIC ***will not*** be:

   - Sold, published, exchanged, or disclosed for commercial purposes.
   - 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.
   - Disseminated to persons not authorized to access or use the information.

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

   - Pursuant to D.C. Official Code §2-534, *et seq.,* the following records will not be provided to the public:

     1. Trade secrets and commercial or financial information obtained from outside the government, to the extent that disclosure would result in substantial harm to the competitive position of the person from whom the information was obtained;

     2. Information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy;

     3. Investigatory records compiled for law-enforcement purposes, including the records of Council investigations and investigations conducted by the Office of Police Complaints, but only to the extent that the production of such records would:

        A. Interfere with:

           ii) Enforcement proceedings;

           iii) Council investigations; or

           iv) Office of Police Complaints ongoing investigations.

B. Deprive a person of a right to a fair trial or an impartial adjudication;

C. Constitute an unwarranted invasion of personal privacy;

D. Disclose the identity of a confidential source and, in the case of a record compiled by a law-enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source;

E. Disclose investigative techniques and procedures not generally known outside the government; or

F. Endanger the life or physical safety of law-enforcement personnel.

4. Inter-agency or intra-agency memorandums or letters, including memorandums or letters generated or received by the staff or members of the Council, which would not be available by law to a party other than a public body in litigation with the public body.

5. Test questions and answers to be used in future license, employment, or academic examinations, but not previously administered examinations or answers to questions thereon;

6. Information specifically exempted from disclosure by statute (other than this section), provided that such statute:

   A. Requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or

   B. Establishes particular criteria for withholding or refers to particular types of matters to be withheld;

7. Information specifically authorized by federal law under criteria established by a presidential executive order to be kept secret in the interest of national defense or foreign policy which is in fact properly classified pursuant to such executive order;

8. Information exempted from disclosure by § 28-4505;

9. Information disclosed pursuant to § 5-417 [information related to arson reports];

10. Any specific response plan, including any District of Columbia response plan, as that term is defined in § 7-2301(1A), and any specific vulnerability assessment, either of

which is intended to prevent or to mitigate an act of terrorism, as that term is defined in § 22-3152(1);

11. Information exempt from disclosure by § 47-2851.06;

12. Information, the disclosure of which would reveal the name of an employee providing information under the provisions of subchapter XV-A of Chapter 6 of Title 1 [§ 1-615.51 et seq.] and subchapter XII of Chapter 2 of this title [2-233.01 et seq.], unless the name of the employee is already known to the public;

13. Information exempt from disclosure by § 7-2271.04;

14. Information that is ordered sealed and restricted from public access pursuant to Chapter 8 of Title 16 of the District of Columbia Code;

15. Any critical infrastructure information or plans that contain critical infrastructure information for the critical infrastructures of companies that are regulated by the Public Service Commission of the District of Columbia; and

16. Information exempt from disclosure pursuant to § 38-2615.

(a-1) (1) The Council may assert, on behalf of any public body from which it obtains records or information, any exemption listed in subsection (a) of this section that could be asserted by the public body pertaining to the records or information.

(2) Disclosure of any public record, document, or information from a District of Columbia government agency, official, or employee to the following persons or entities shall not constitute a waiver of any privilege or exemption that otherwise could be asserted by the District of Columbia to prevent disclosure to the general public or in a judicial or administrative proceeding:

(A) The Council;

(B) A Council committee;

(C) A member of the Council acting in an official capacity;

(D) The District of Columbia Auditor; or

(E) An employee of the Office of the District of Columbia Auditor.

(b) Any reasonably segregable portion of a public record shall be provided to any person requesting the record after deletion of those portions which may be withheld from disclosure pursuant to subsection (a) of this section. In each case, the justification for

the deletion shall be explained fully in writing, and the extent of the deletion shall be indicated on the portion of the record which is made available or published, unless including that indication would harm an interest protected by the exemption in subsection (a) of this section under which the deletion is made. If technically feasible, the extent of the deletion and the specific exemptions shall be indicated at the place in the record where the deletion was made.

(c) This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from the Council of the District of Columbia. This section shall not operate to permit nondisclosure of information of which disclosure is authorized or mandated by other law.

(d) The provisions of this subchapter shall not apply to the Vital Records Act of 1981.

(e) All exemptions available under this section shall apply to the Council as well as agencies of the District government. The deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege are incorporated under the inter-agency memoranda exemption listed in subsection (a)(4) of this section, and these privileges, among other privileges that may be found by the court, shall extend to any public body that is subject to this subchapter.

Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606, and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

- Information exempt from disclosure pursuant to D.C. Official Code §2-1707.
- Information exempt from disclosure pursuant to D.C. Official Code §4-1305.08.
- Information exempt from disclosure pursuant to D.C. Official Code §5-113.06.
- Information exempt from disclosure pursuant to D.C. Official Code §7-1605.
- Information exempt from disclosure pursuant to D.C. Official Code §14-307.
- Information exempt from disclosure pursuant to D.C. Official Code §§16-2331-2336.
- Information exempt from disclosure pursuant to D.C. Official Code §16-2394.
- Information of personally identifiable health information pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or any other confidentiality law.

- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission.

- A violation of an authorized nondisclosure agreement.

10. The NTIC 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.

K. Redress

K.1 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 Subsection 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 NTIC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The center's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

2. The existence, content, and source of the information will not be made available by the NTIC to an individual when the information is exempt from disclosure pursuant to D.C. Official Code §2-534 and Section J, 9 and:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.
   - Disclosure would endanger the health or safety of an individual, organization, or community.
   - The information is in a criminal intelligence information system subject to 28 CFR Part 23 [*see* 28 CFR § 23.20(e)].
   - The information is exempt from disclosure pursuant to the provisions in J.9 and E.3.
   - The information source does not reside with the center.
   - The center did not originate and does not have a right to disclose the information.
   - Other ***authorized*** basis for denial.

   If the information does not originate with the center, 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.

K.2 Corrections

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

K.3 Appeals

1. 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 NTIC 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. Official Code § 2-537.]

K.4 Complaints

1. If an individual has a complaint regarding 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,
        i) Is held by the NTIC and
        ii) 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 the following address: NTIC_privacy@dc.gov.

    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 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 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 by the center of all complaints and the resulting action taken in response to the complaint.

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

L. Security Safeguards

1. The NTIC's Security Officer is designated and trained to serve as the center's security officer.

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

3. The NTIC 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.

4. The NTIC 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.

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

6. The audit log of queries made to the NTIC will identify the user initiating the query.

7. The NTIC will utilize watch logs to maintain audit trails of requested and disseminated information.

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

9. The NTIC will follow the data breach notification guidance set forth in OMB Memorandum M-07-16 (May 2007, see http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.)

   The NTIC will immediately notify the originating agency from which the center received personal information of a suspected or confirmed breach of such information.

M. Information Retention and Destruction

1. All applicable information will be reviewed for record retention (validation or purge) by NTIC every five (5) years, as provided by 28 CFR Par 23.

2. When information has no further value or meets the criteria for removal according to the NTIC's retention and destruction policy, it will be purged, destroyed, and deleted or

returned to the submitting (originating) agency.

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

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

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

6. A record of information to be reviewed for retention will be maintained by the NTIC, 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.

N. Accountability and Enforcement

N.1 Information System Transparency

1. The NTIC will be open with the public regarding information and intelligence collection practices. The center's privacy policy will be provided to the public for review, made available upon request, and posted on the center's Web site at www.NTIC.dc.gov.

2. The NTIC'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: NTIC_privacy@dc.gov.

N.2 Accountability

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

2. The NTIC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of 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 NTIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this

policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least semiannually and a record of the audits will be maintained by the Privacy Officer of the center.

4. The NTIC'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 C.3]

5. The NTIC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). 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 staffof the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s)

6. The NTIC will regularly communicate with the designated representatives from agencies comprising the Executive Board of Directors. The 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.

N.3 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 NTIC will:
   - Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
   - Suspend, demote, transfer, or terminate center personnel, as permitted by applicable personnel policies.
   - Apply administrative actions or sanctions as provided by D.C. Official Code § 2-537; D.C. Official Code §§16-2336; 16-2394; General Order 120.21 and other pertinent regulations as provided in agency and center personnel policies.
   - If the authorized user is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy

2. The NTIC 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.

O. Training

1. The NTIC will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy:
   - All assigned personnel of the center.
   - Personnel providing information technology services to the center.
   - Staff in other public agencies or private contractors providing services to the center.
   - Users who are not employed by the center or a contractor.

2. The NTIC 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.

3. The NTIC'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 center.
   - 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 center privacy protection policies and procedures.
   - The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

Appendix A – Terms and Definitions

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

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

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

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

Agency—HSEMA and all agencies that access, contribute, and share information in the HSEMA's justice information system.

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

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

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

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

Center—Refers to the [name of fusion center] and all participating state agencies of the NTIC.

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

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, 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.

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

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

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

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

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

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions;

transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] identifier, or booking or detention system number). Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

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

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

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

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

Protected Information—Protected information includes Personal Information about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the District of Columbia Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23, applicable state and tribal constitutions; and applicable state, local, and tribal laws 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 center's information.

Media organizations.

Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the center or participating agency.

Public does not include:

Employees of the center or participating agency.

People or entities, private or governmental, who assist the center in the operation of the justice information system.

Public agencies whose authority to access information gathered and retained by the center is specified in law.

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

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

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

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

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

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

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.

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.

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

Appendix C – Suspicious Activity Reporting (SAR) Summary of Provisions

For fusion centers that are continuing to formulate or may have already completed a privacy policy using this template prior to the inclusion of SAR provisions, a summary of the updated provisions specific to the SAR process is provided within this appendix. Section headings and numbering are retained for template reference purposes. Please note that other provisions contained within this template may also apply to SAR information.

Appendix D – Federal and District of Columbia Statutes

U.S. Constitution, First Amendment

First Amendment Rights and Police Standards, D.C. Official Code §§5-331-01-337.01

D.C. Official Code §1-615.51

D.C. Official Code §2-1707

D.C. Official Code §§2-531-537

D.C. Official Code §2-5417

D.C Official Code §4-1305.08

D.C. Official Code §5-113.06

D.C. Official Code §5-417

D.C. Official Code §7-1201.02

D.C. Official Code §7-1605

D.C. Official Code §7-2301

D.C. Official Code §7-2271

D.C. Official Code §14-307

D.C. Official Code §16-2331-2336

D.C. Official Code §16-2393-2394

D.C. Official Code §22-3152

D.C. Official Code §28-4505

D.C. Official Code §44-801

D.C. Official Code §47-2851.06

General Order 120.21