NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM – PRIVACY POLICY

I. STATEMENT OF PURPOSE

The mission of HSEMA is to ensure that the District of Columbia (District) is prepared to prevent, protect against, respond to, mitigate and recover from all threats and hazards. As part of this mission, HSEMA overseas the National Capital Region Threat Intelligence Consortium ("NTIC"), which is the District's fusion center. The purpose of this policy is to establish privacy guidelines for the NTIC. The NTIC analyzes available data in order to help detect, prevent, and respond to terrorist and other threats to public safety, as well as to facilitate information sharing during any event requiring an emergency response, primarily within the District of Columbia and secondarily, the National Capitol Region (NCR).

II. POLICY APPLICABILITY AND LEGAL COMPLIANCE

All assigned personnel in the NTIC and service users will comply with the NTIC privacy policy concerning the information the Center collects, receives, maintains, archives, accesses or discloses to center personnel, government agencies; including agencies participating in the Information Sharing Environment (ISE), participating criminal justice and public safety agencies, as well as to private contractors and the general public.

The NTIC will provide a printed copy of this policy to all assigned personnel in the NTIC and will require them to sign a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains. All Service users will be required to review this policy and acknowledge their compliance with the policy through their signature on the Non-Disclosure Agreement (NDA). This privacy policy is located on the District of Columbia Homeland Security and Emergency Management Agency (HSEMA)/NTIC website (http://hsema.dc.gov).

All NTIC personnel, HSEMA personnel, participating agency personnel (to include Liaison Officers (LNOs)), private contractors, and other authorized users will comply with all applicable laws, regulations, and rules protecting privacy, civil rights, and civil liberties, including but not limited to those listed in Section V, Part B of this policy.

All of NTIC's criminal intelligence files meeting the standards of collection by the NTIC will comply with all internal operational policies and be retained in compliance with Title 28, Code of Federal Regulations (C.F.R.), Part 23, the Fusion Center Guidelines and any applicable state or local statutes governing the collection, dissemination, retention, receipt, maintenance, access, and destruction of information. The NTIC internal operational policies comply with applicable laws referenced in previous paragraph.

III. GOVERNANCE AND OVERSIGHT

On April 1, 2012, Mayor's Order 2012-37 designated HSEMA as the "primary fusion center for the District of Columbia." Further, Mayor's Order 2012-204, vested HSEMA with "[a]dministrative control and the day to day operations…" of the NTIC, which is the internal entity responsible for carrying out the fusion center functions. 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 Executive Director of the Center.

Pursuant to Mayor's Order 2012-204, the NTIC receives advice and guidance from the District of Columbia Fusion Center Advisory Board (the Board). The Board's purpose is to "develop a proposed operational framework for the…" the NTIC.

That operational framework includes "policies that are designed to ensure that individuals' constitutional rights, civil liberties, civil rights and privacy interests are protected at all times." In that regard HSEMA and NTIC will submit substantive policies to the Advisory Board for review and comment.

In a further effort to safeguard the privacy, civil rights, and civil liberties of the public, the NTIC is guided by a trained Privacy Officer who is designated by the Director of HSEMA. The Privacy Officer is responsible for handling reported errors and violations, ensuring the provision of training under Section V, Part M of this policy, and, will ensure that the Center adheres to the provisions of the ISE Privacy Guidelines and other requirements for participation in the ISE. The Privacy Officer will ensure that the enforcement procedures and sanctions outlined in Section V, Part K (Accountability and Enforcement) of this policy are adequate and enforced to the extent necessary. The Privacy Officer is also responsible for the development of the privacy policy and annual review. The Privacy Officer can be contacted at the following address, NTIC@dc.gov, Attention: Privacy Officer.

IV. DEFINITIONS

Authorized User refers to an individual who is trained in the use of intelligence systems and has been provided appropriate access.

C.F.R. is the Code of Federal Regulations.

Criminal Intelligence Information is 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. Part 23.

Information Sharing Environment (ISE) is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of state, local, and tribal agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR) is 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).

Law as used in this policy includes any local, state, tribal, territorial, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order.

Need to Know applies when, 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.

Personal data refers to any personally identifiable information that relates to an identifiable individual.

Protected Information includes personal data about individuals 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. Part 23; and applicable state laws and local ordinances. Protection may also be extended to organizations by fusion center or state local, or tribal agency policy or regulation.

Public includes: (a) any person and any for-profit or nonprofit entity, organization, or association; (b) any governmental entity for which there is no existing specific law authorizing access to NTIC information; (c) media organizations; and (d) 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 NTIC.

Public does not include: (a) employees of NTIC; (b) people or entities, private or governmental, who assist NTIC in the operation of the justice information system; and (c) public agencies whose authority to access information gathered and retained by NTIC is specified in law.

Qualified Individual is a person who has received appropriate training and has been provided necessary access in order to perform their duties.

Right to Know is based on having legal authority or responsibility or when, 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.

Role Based Access is a type of access authorization that uses roles to determine access rights and privileges.

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

Suspicious Activity Report (SAR) is official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. 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.

V. OPERATING PRINCIPLES

A. Seeking and Retaining Information

The NTIC will seek or retain only information concerning: an individual or group reasonably suspected of criminal conduct or activity (including terrorism); 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 is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches). The NTIC will ensure that the source of the information sought or retained is reliable and verifiable, or limitations on the quality of the information are identified. No information will be gathered or collected by the NTIC in violation of federal, state, or local laws or regulations.

The NTIC will not seek or retain any information and originating agencies will agree not to submit information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicities, citizenships, places of origin, ages, disabilities, genders, or sexual orientations.

The NTIC 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 NTIC will adhere to the following practices regarding the receipt, collection, assessment, storage, access, dissemination, and retention of tips, leads, and suspicious incident reports: (a) the information received is assessed upon receipt for sensitivity and confidence and is treated appropriately; (b) the information is evaluated and investigated by trained personnel to determine its credibility, value, and appropriate categorization; (c) the information is stored and maintained in a secure environment with limited access and is labeled to delineate it from other information; (d) the information is only accessible to, and may be disseminated by, authorized personnel using the standards that meet the reasonable suspicion requirement; and (e) the information will be retained using the applicable retention schedule. The NTIC will keep a record of the source of all information collected.

B. Methods of Seeking or Receiving Information

Information gathering, and investigative techniques used by NTIC will comply with the applicable provisions of the U.S. Constitution, federal and local laws and guidelines that protect the privacy, civil rights, and liberties of citizens. These include, but are not limited to: the Bill of Rights (the first ten (10) amendments to the U.S. Constitution); the Privacy Act of 1974 (5 U.S.C. § 522a); the Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-2522, 2701-2709, 3121-

3125); 28 C.F.R. Part 23 (regarding criminal intelligence information systems); the First Amendment Assemblies Act of 2004 (D.C. Code §§ 5-331.01-5-331.17); the District of Columbia Freedom of Information Laws (D.C. Code §§ 2-531-2-537); the Department of Homeland Security's Fair Information Practice Principles (FIPPs)(*see* DHS Memorandum No. 2008-1), and the criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan.*

NTIC will not directly or indirectly receive, seek, accept, or retain information from an individual who may receive a fee or benefit for providing the information, if the Center knows or has reason to believe that: (a) the individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to NTIC; (b) the individual or information provider used methods for collecting the information that NTIC itself could not legally use; (c) the specific information sought from the individual or information provider could not legally be collected by NTIC; or (d) the Center has not taken the steps necessary to be authorized to collect the information. Non-government information providers under contract to provide information must demonstrate that they have appropriate safeguards and privacy policies in place.

C. Classification of Information Regarding Validity and Reliability

At the time of retention in the system, information will be categorized regarding the: (a) type of information (tips/leads, SARs, criminal intelligence information, etc.); (b) nature of the source; (c) reliability of the source; and (d) sensitivity of the information.

The categorization and labeling of retained information will be re-evaluated when: (a) new information is gathered that has an impact on the validity and reliability of retained information; or (b) there is a change in the use of the information affecting access or disclosure limitations; or (c) per scheduled retention reviews.

D. Classification of Information Regarding Limitations on Access and Disclosure

At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations identified in 28 C.F.R. Part 23 and the D.C. Code regarding access and sensitivity of disclosure in order to: (a) protect confidential sources and police undercover techniques and methods; (b) not interfere with or compromise pending criminal investigations; (c) protect an individual's right of privacy and civil rights; and (d) provide legally required protection based on the status of an individual as a juvenile, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

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

- The information is protected information, including personal data on any individual (*see* Section IV (Definitions)) and, to the extent expressly provided in this policy, organizational entities.

- The information is subject to District of Columbia and federal law restricting access, use, or disclosure.

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.

The classification of existing information will be re-evaluated whenever: (a) new information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or (b) there is a change in the use of the information affecting access or disclosure limitations.

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. 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.

- Use a standard reporting format and data collection codes for SAR information.

- Store the information using the same storage method used for data which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.

- Allow access to or disseminate the information using the same 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 from law enforcement, homeland security, or for public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.

- Retain information for up to two years in order to investigate a tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, no further action, assigned, ongoing, completed) so that a subsequent authorized user knows the status and purpose of the retention and will retain the information based on the retention period associated with the disposition label.

- Adhere to and follow PSP 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.

NTIC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems that are 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.

NTIC will identify and review protected information that may be accessed or disseminated by the Center prior to sharing that information through the Information Sharing Environment. Further, NTIC 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.

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

E. Information Quality

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 V, Part G (Merging Records)) has been met. 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)).

Originating agencies, external to HSEMA, are responsible for reviewing the quality and accuracy of the data provided to the NTIC. The NTIC 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.

The NTIC will advise recipient agencies in writing when information previously provided to them is deleted or changed 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.

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.

The NTIC will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system. The NTIC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that information will be deleted from the system when the agency learns that: (a) the information is erroneous, misleading, obsolete, or otherwise unreliable; (b) the source of the information did not have authority to gather the information or to provide the information to the agency; or (c) the source of the information used prohibited means to gather the information.

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

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

Information-gathering and investigative techniques used by the NTIC and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information they are authorized to seek or retain.

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.

F. Collation and Analysis of Information

Types of information available for analysis include investigative, intelligence, open source, and public records (*see* Section V, Part A). Information will only be analyzed by qualified individuals (*see* Section IV) to: (a) Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the Center; (b) Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities; (c) 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 NTIC Advisory Board; (d) Protect and mitigate all-source threats against District of Columbia critical infrastructure as designated by the City.

NTIC personnel will comply with laws regarding privacy, civil rights, and civil liberties as outlined in Section II.

The NTIC requires that all appropriate written analytical products be reviewed and approved by the Privacy Officer or in the Privacy Officer's absence, by the Privacy Officer's designee, to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination by the Center.

G. Merging Records

Information about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifying information sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of a match. Partial matches of information will be accompanied by a clear statement that it has not been established that the information relates to the same individual and, if matched, will contain a clear statement that it has been adequately established that the information relates to the same individual or organization.

Criteria for determining matches 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.

H. Sharing and Disclosing of Information

Credentialed, role-based access criteria will be used to control: (i) what information a class of users can have access to; (ii) what information a class of users can add, change, delete or print; and, (iii) to whom the information can be disclosed and under what circumstances.

Information gathered or collected and records retained by NTIC will only be accessed by, or disclosed to, persons within the criminal justice system, persons within the NTIC or in other governmental agencies who are authorized to have access and receive protected information, only for legitimate law enforcement, public prosecution, or justice purposes and only in the performance of official duties in accordance with the 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 or received information retained by NTIC and the nature of the information accessed will be kept by the Center.

Information gathered or collected, and records retained by 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 five (5) years by NTIC.

Information gathered or collected, and records retained by NTIC may be accessed or disseminated to those individuals responsible for public protection, public safety, or public health only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property. An audit trail sufficient to allow the identification of each individual who accessed information or received information retained by NTIC and the nature of the information accessed will be kept by NTIC.

Information gathered or collected, and records retained by 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 NTIC 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.

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

- Information exempt from disclosure under D.C. Code § 2-534 (2013);
- 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);
- Information exempt from disclosure pursuant to D.C. Code § 2-1707 (2013);
- Information exempt from disclosure pursuant to D.C. Code § 4-1305.08 (2013);
- Information exempt from disclosure pursuant to D.C. Code § 5-113.06 (2013);
- Information exempt from disclosure pursuant to D.C. Code § 7-1605 (2013);
- Information exempt from disclosure pursuant to D.C. Code § 14-307 (2013);
- Information exempt from disclosure pursuant to D.C. Code §§ 16-2331 to 16-2336 (2013);
- Information exempt from disclosure pursuant to D.C. Code §16-2394 (2013);
- 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;

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

- A record that, if disseminated, would violate an authorized nondisclosure agreement.

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.

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

Information gathered or collected and records retained by the NTIC will not be: (i) sold, published, exchanged, or disclosed for commercial purposes; (ii) 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; (iii) Disseminated to persons not authorized to access or use the information.

I. Redress

To the extent permitted under the District of Columbia's Freedom of Information Act (FOIA Act), D.C. Code § 2-531, *et seq.*, and upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified below, an individual may be entitled to know the existence of and to review the information about him or her that has been gathered and retained by NTIC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (*i.e.*, making corrections). The NTIC's response to the request for information will be made within the time requirements set forth in the FOIA Act and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

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

- The information is exempt from disclosure pursuant to any of the legal authorities outlined above in Section V, Part E (Sharing and Disclosing of Information);

- 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 information system subject to 28 C.F.R. Part 23;

- The information source does not reside with NTIC or NTIC did not originate the information and does not have a right to disclose it;

- Any other authorized basis for denial exists.

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

If an individual requests correction of information *originating with 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.

The individual who has requested disclosure will be given reasons if disclosure or requests for corrections are denied by NTIC. The individual will also be informed of the procedure for appeal set forth in the FOIA Act (*See* D.C. Code § 2-537) when NTIC 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.

If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

(a) is exempt from disclosure,

(b) has been or may be shared through the ISE,

(1) is held by NTIC and

(2) allegedly has resulted in demonstrable harm to the complainant,

the individual shall submit a detailed written letter, by mail, setting forth his/her complaint regarding the accuracy and/or completeness of the information to NTIC's Privacy Officer at the following address:

D.C. Homeland Security Management Agency,
National Capital Region Threat Intelligence Consortium,
Attention: Privacy Officer
2720 Martin Luther King, Jr. Avenue, SE,
Washington, D.C. 20032.

Complaints can also be received by the Privacy Officer via the following email address: NTIC@dc.gov, Attention: Privacy Officer.

The Privacy Officer will acknowledge the complaint and state that it will be reviewed but not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with NTIC, the Privacy Officer will notify the originating agency in writing or electronically within ten (10) business 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 NTIC that is the subject of a complaint will be reviewed within 30 business 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 business days, NTIC will not share the information until such time as the complaint has been resolved. A record will be kept by NTIC of all complaints and the resulting action taken in response to the complaint.

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

J. Information Retention and Destruction

Consistent with the provisions of 28 C.F.R. Part 23, criminal intelligence information and SARs retained by NTIC are reviewed for purging at least every five years. 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. Further, when information has no further value or meets the purge criteria under applicable NTIC administrative regulations, applicable District law, or 28 C.F.R. Part 23 (for criminal intelligence information systems), it will be purged, destroyed, deleted, or returned to the submitting source.

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. 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. 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.

Pursuant to 28 C.F.R. Part 23, as applicable, NTIC will purge criminal intelligence information under the following conditions: (a) the data is no longer relevant or necessary to the goals and objectives of the NTIC; (b) the data has become obsolete, making it unreliable for present purposes and the utility of updating the data would be worthless, or (c) the data cannot be utilized for strategic or tactical intelligence studies.

K. Accountability and Enforcement

This Privacy Policy is available upon request and also available to the public on the (HSEMA)/NTIC website (http://hsema.dc.gov/publication/washington-regional-threat-analysis-center-privacy-policy).

NTIC's Privacy Officer is 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 NTIC. The Privacy Officer ensures that enforcement procedures and sanctions outlined in this Privacy Policy are adequate and enforced to the extent necessary. Any complaints or reports of violations of department policies by NTIC personnel will be handled through appropriate internal HSEMA policies and procedures. Inquiries or complaints that are received by the Privacy Officer involving non-NTIC personnel will be directed to the Executive Director of the Center who will report the matter to the employee's agency.

The Privacy Officer can be contacted, via email, at NTIC@dc.gov, Attention: Privacy Officer.

NTIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the system itself within 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 conducted by the Privacy Officer, at least semi-annually, and he/she will maintain a record of the audits. The NTIC 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.

The NTIC will conduct periodic audits and inspections of the information and intelligence contained in its information system(s). The audits will be conducted by the Privacy Officer or a designated independent panel, which can be convened at the Advisory Board's discretion. The Privacy Officer or the independent panel, if convened, has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of NTIC. The audits will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the Center's information and intelligence system(s).

The NTIC's Advisory Board, guided by the designated 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.

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.

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 Center's privacy policy.

If a user is suspected of or found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, HSEMA and/or the NTIC will: (a) suspend or discontinue access to information by the user; (b)

suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies; (c) apply other sanctions or administrative actions as provided in agency personnel policies; (d) request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or (e) refer the matter to appropriate authorities for criminal prosecution, as necessary.

L. Security Safeguards

The NTIC has Security Officer who was designated by the Director of HSEMA. The Security Officer shall receive appropriate training regarding the safeguarding and security of information. The Security Officer shall report all errors or violations of this policy to the Privacy Officer and the Center's Executive Director. Together they will ensure that enforcement procedures and sanctions outlined within this Privacy Policy are adequate and enforced.

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 NTIC's databases from outside the facility will be allowed only over secure networks.

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 the Criminal Intelligence Systems Operating Policies, 28 C.F.R. §§ 23.1-23.40 (2012).

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.

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.

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

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

The NTIC will follow the data breach notification guidance set forth in Office of Management and Budget, Memorandum M-07-16,
https://www.whitehouse.gov/sites/default/files/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. Training

NTIC will require the following individuals to participate in introductory, and thereafter, annual training programs regarding the implementation of and adherence to this Privacy Policy: (a) all

NTIC assigned personnel, including interns and liaison officers (LNOs); (b) staff in other public agencies or private contractors providing services to the Center; (c) Personnel providing information technology services to the Center; (d) Users who are not employed by the Center or contractors; and, (e) any person who physically transits the center spaces on a recurring basis or physically works closely with Center personnel inside the NTIC 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 Center personnel and systems.

The training program will cover: (a) any applicable federal or state statute, or any NTIC regulation concerning privacy, civil rights, and civil liberties protection; (b) substance and intent of the provisions of this Privacy Policy relating to collecting, use, analysis, retention, destruction, sharing, and disclosure of information retained by NTIC; (c) the impact of improper activities associated with information accessible within or through NTIC; (d) the nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any; and (e) PSP's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the ISE.

In particular, all personnel listed in Paragraph 1 of this Section will be required to complete the online training regarding 28 C.F.R. Part 23, *et seq.*, which is provided by U.S. Department of Justice's Bureau of Justice Assistance. The NTIC Administrative Assistant will maintain a record of this training.

DISTRICT OF COLUMBIA HOMELAND SECURITY AND EMERGENCY MANAGEMENT AGENCY:

Date: 5/31/2019

Dr. CHRISTOPHER RODRIGUEZ
DIRECTOR, HSEMA