Privacy Protection Policy and Constitutional Protections Advisory Board

1. Subject: Privacy Protection Policy and the Constitutional Protections Advisory Board

2. Purpose: To establish written policies and procedures for the protection of individuals' and organizations' privacy rights, civil rights, and civil liberties, regarding information contained within the Maryland Coordination and Analysis Center (MCAC). Further, to define duties of the MCAC Constitutional Protections Advisory Board (CPAB) to monitor compliance with this policy and to advise the Executive Committee of the U. S. Department of Justice (DOJ) established Anti-Terrorism Advisory Council (ATAC) Executive Committee, which consists of the Chief Executives of the U.S. Attorney's Office, Federal Bureau of Investigation, U.S. Immigration and Customs Enforcement, MD Sheriffs' Association, MD Police Chiefs' Association, MD Health Officer's Association, MD Military Department, MD Homeland Security Advisor, U.S. Coast Guard, MD Fire Chief's Association, 2 "Major Jurisdiction" Police Chiefs, MD State Police, MD Metro Fire Chief's Association, MD Fireman's Association, MD Transportation Authority Police, and the Police Chief of the jurisdiction that provides one of the three key managers to the MCAC, and which governs MCAC policy and operational philosophy, on such matters that it may deem to be appropriate.

3. Applicability: This policy applies to all assigned personnel within MCAC, those working under contract with the MCAC, and to those who use its services (Users). All affected personnel will be provided a written or electronic copy of this policy through the most efficient means available at the time of distribution and will sign a written acknowledgement of receipt of this policy and agreement to comply with the applicable provisions it contains. This policy applies to information the MCAC 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 other entities and individuals receiving MCAC generated information that is not public information.

4. Policy: The MCAC, and participating agencies, employees, and users will comply with all applicable laws and regulations protecting individuals' and organizations' privacy rights, civil rights, and civil liberties in the use, analysis, retention, destruction, sharing and disclosure of protected information received and stored within the MCAC. In sharing and disclosing such information, the MCAC also will take reasonable measures to ensure the sources and methods of information gathering are adequately protected. The MCAC has adopted internal operating policies and procedures that are in compliance with applicable law protecting privacy, civil rights, and civil liberties. A list of definitions used in the policy and a list of applicable law may be found in Appendices A and B, respectively.

   The policy set forth herein is not intended to create or confer any rights, privileges, or benefits in any matter, case, or proceeding, see United States v. Caceres, 440 U.S. 741 (1979), and does not have the force of law.

5. Accountability for Activities: Primary responsibility for the operation of the MCAC information systems, including operations, the seeking, receiving, retention, evaluation, analysis, sharing, disclosure of, and destruction of information, and enforcement of this policy is assigned to the Director, MCAC which is appointed by the ATAC. At a minimum, the Director will:

a. Establish policies, procedures, and practices that use software, information technology tools, and physical security measures to protect information from unauthorized access, modification, theft or sabotage;

b. Designate a facility security officer, who will be properly trained in physical security procedures to ensure the protection of information stored by the MCAC;

c. Store information in a manner that cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions;

d. Require individuals authorized to access MCAC's systems to agree in writing to comply with the provisions of this policy;

e. Adopt and follow procedures to evaluate the compliance of MCAC information system users with system requirements, this policy, and applicable law. This will include logging access to these systems and periodically conducting audits of the information receipt, analysis, dissemination, and storage processes addressed in this policy memorandum. The audits will be conducted at least annually and randomly by a designated representative of the MCAC, be maintained by the Privacy Officer, and be subject to review by a designated representative of the ATAC Executive Committee. The audits will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the information;

f. Provide audit results, and as necessary, a list of corrective actions taken to remedy identified deficiencies, to the MCAC Constitutional Protections Advisory Board and the ATAC Executive Committee;

g. Designate and provide adequate training for an MCAC Privacy Officer, who will receive reports regarding alleged errors and violations of the provisions of this policy. The Privacy Officer will receive and coordinate complaint resolution, and serve as the liaison for the Information Sharing Environment, ensuring privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy related technologies. The Privacy Officer can be contacted at the following address: mdwatch@mcac.maryland.gov. The MCAC Privacy Officer ensures that enforcement procedures and sanctions outlined in section (aa) of this policy are adequate and enforced.

6. Procedure:

a. Seeking & Retaining Information: The MCAC will only seek and/or retain information on individuals and organizations to corroborate and/or validate tip or lead information (including SAR information) or when there is reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is planning criminal conduct or activity (including terrorism) that presents a threat to any individual, the community, or the nation, and the information is relevant to the criminal conduct or activity. Further, the MCAC will only seek information on individuals and organizations in support of field operating elements engaged in an ongoing law enforcement investigation or event, and/or information that does not contain personally identifiable information for non-law enforcement agencies/entities for health and public safety purposes (unless there is an imminent danger to life or property).

The MCAC will not seek information and information-originating agencies will agree to not submit information about individuals or organizations solely on the basis of their religious, social or political views or activities, their participation in a particular noncriminal organization or lawful event, race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

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

- The information is "protected information," to include Personal Information on any individual (see Appendix A, Definitions) and, to the extent expressly provided in this policy, includes organizational entities.

- The information is subject to federal (or state) law restricting access, use, or disclosure. Information-gathering (acquisition) and access and investigative techniques used by the MCAC 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.
    - Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP).
    - Constitutional provisions; Federal laws and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

Information gathering techniques used by the MCAC will, and those used by originating agencies should, be no more intrusive or broad in scale than is necessary in the particular circumstance to gather information it is authorized to seek or retain.

Nothing in this section shall be construed to limit the ability of the MCAC to initiate, without a specific request, short term research or information gathering regarding events or activities being publicly reported in the media which may impact on the health and public safety of the State of Maryland and its residents.

Further, nothing in this policy shall prohibit the MCAC from gathering and/or retaining information that is routinely collected by public safety agencies in the lawful performance of their duties.

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

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

The MCAC will not directly or indirectly receive, seek, accept, or retain information from: 1) 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, or 2) A commercial information provider that is legally prohibited from obtaining or disclosing the information.

b. Limitations on Access to and Disclosure of Information: The MCAC will limit access to and disclosure of personally identifiable information it has obtained concerning individuals and organizations to those personnel who are directly involved in the authorized use of the information. Access is granted and/or disclosure permitted only to authorized individuals who must adhere to the policy and procedures stated herein. Only limited information access is granted and/or disclosure permitted in order to ensure that the MCAC:

    1) Protects an individual's right to privacy, civil liberties, and civil rights;

    2) Does not interfere with or compromise pending criminal investigations (including terrorism), to include protecting confidential sources and investigative techniques and methods;

3) Provides legally required protection based upon the status of an individual (i.e. – the participant in a substance abuse or mental health treatment program)

In furtherance of the items listed above, the MCAC will not disclose nor allow records or information to be:

4) Sold, published, exchanged, or disclosed for commercial purposes

5) Disclosed or published without prior notice to the originating agency, unless disclosure is agreed to as part of the normal operations of the agency

6) Disseminated to persons not authorized to access or use the information

c. Access Controls and Security for Information Retained by the MCAC: Credentialed, role-based access criteria will be used by the MCAC, as appropriate, to control:

1) The information to which a specified group of users has access;

2) The information a specified group of users can add, change, delete, or print; and

3) To whom, individually, the information can be disclosed, and under what circumstances.

d. Security Safeguards: The MCAC will operate in a secure facility. Internal and external safeguards will be used to prevent network intrusions. As such the following applies:

1) The MCAC 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.

2) Information will be stored in a manner that only authorized personnel can access, modify, delete, or destroy it.

3) Access to MCAC 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 (as specified in section 6 (bb) of this policy) accordingly.

4) The identities of persons making queries of the MCAC's data applications are recorded in a manner that establishes an audit trail. .

5) To prevent unauthorized disclosure, publicly available data and sensitive data, such as risk and vulnerability assessments or data containing Personally Identifiable Information (PII), will be stored separately.

e. Collection, Collation, And Analysis Of Information: Information identified in section 6(a) of this policy that is sought or received by the MCAC or from other sources will only be subject to collation and analysis to:

1) Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal or terrorist activities generally; or

2) Further crime (including terrorism) prevention, enforcement, force deployment, or prosecution objectives and priorities established by the ATAC Executive Committee and MCAC management.

f. Persons Authorized to Evaluate and Analyze Information Obtained by the MCAC:

1) Information may only be processed and/or analyzed by MCAC staff who have been properly trained and obtained the appropriate clearances to do so as specified in section 6 (bb) of this policy.

g. Evaluation and Labeling of Information: All information developed by the MCAC, and products originating and/or retained in the MCAC, will be evaluated and labeled with attention to privacy concerns as follows:

1) All information received by the MCAC, except information specified in section 6 (m) of this policy, will be assessed to determine its nature, quality, and usefulness. Upon assessment, the information will be categorized to reflect the assessment and appropriately labeled with the following information and as outlined in Information Collection, Analysis, Dissemination, Retention and Destruction Policy:

a. 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.

b. Nature (credibility and reliability) of the source based on occupation, background, or previous reporting

c. Age of information

d. Accuracy of information

e. Completeness of information

f. Validity (verifiability of information)

2) In the event new information is obtained, where the MCAC has received previous information, the original information will be re-evaluated in the context of the new and re-labeled as needed.

3) Alleged or suspected errors pertaining to information held by the MCAC will result in a re-evaluation and errors will be corrected, in consultation with the originating agency when appropriate, as needed. In the event errors cannot be addressed or corrected, the information will be purged in accordance with section 6 (w) of this policy.

4) MCAC personnel will record the source of all information sought and collected by the Center.

5) All information originating from the MCAC, unless otherwise evaluated, will be considered to contain Personally Identifiable Information as defined in Appendix A of this policy. As such, all MCAC generated products will include a statement indicating the following:

a. “This document contains Personally Identifiable Information. This information may be subject to Federal, State, and local laws regarding its use and dissemination.”

6) All information distributed by the MCAC, including terrorism-related information shared through the ISE, will be labeled, at a minimum, with the following information:

a. Name of the originating center, organization or agency, component and subcomponent

b. Date the information was collected and date the accuracy was last verified

c. Title and contact information of person providing information, or point of contact for questions about the information, to include accuracy of the information.

7) The MCAC will ensure all information is labeled (or ensure that the originating agency has labeled information) with any legal restrictions on information sharing based on information sensitivity or classification that may pertain to its use and dissemination, to include information with special handling procedures.

8) At the time a decision is made by MCAC 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 his or her 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.

h. Re-Evaluation of Information: Periodic re-evaluation of information may be required to ensure its quality is consistent with the standards set forth in this and related policies. Re-evaluation will occur in the following situations:

1) In the event new information is obtained, where the MCAC has received previous information, the original information will be re-evaluated in the context of the new and re-labeled as needed. The center will 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.

2) Alleged or suspected error pertaining to information received or produced by the MCAC will result in a re-evaluation and errors will be corrected as needed.

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

4) In the event an error has been identified in information received or produced by the MCAC that has resulted in the issuance of an alert, bulletin, or other intelligence product, a follow-up report will be issued to address the error in information, and the new product will be disseminated to all original recipients. If an error causes the credibility of an MCAC generated report to become questionable, a statement will be issued rescinding the report.

5) MCAC will conduct periodic data quality reviews of information originating within the MCAC in accordance with the Center's Information Collection, Analysis, Dissemination, Retention and Destruction Policy and will determine its continued relevance and applicability for which it was

collected 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).. In the event the information is considered to be incorrect, no longer relevant, or applicable, the information will be destroyed, deleted, or purged in accordance with the Information Retention and Destruction (Section 6 (w)) portion of this policy. MCAC 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.

i. Merging of Information: The following guidelines will be followed when merging, or combining, information received by the MCAC:

   1) Records of individuals and/or entities may only be merged when information reasonably indicates a match of the records. All available information must be considered prior to merging records. The information used to determine a match in records may include, but is not limited to, name, date of birth, social security number, addresses, scars, tattoos, tax ID number, and telephone numbers.

   2) When sufficient information is available to suspect a match in records which is not supported by additional information, the records will remain independent, but may be linked with a statement indicating a definite match between the records has not been identified.

j. Review of Information Generated by the MCAC: All documents, including analytical products (as cited in 6. e.), generated by the MCAC will undergo an editorial and substantive review through MCAC management in accordance with the Information Collection, Analysis, Dissemination, Retention and Destruction Policy prior to publication. In addition, the following guidelines will be followed:

   1) All MCAC staff shall be trained in privacy concerns and applicable rules, regulations, and laws, as they relate to reporting. Reviewers at all levels will attempt to ensure any privacy issues identified during the review process are identified and addressed prior to submission to the next reviewing official.

   2) The MCAC Privacy Officer will review all analytical products to ensure proper privacy, civil rights, and civil liberties protections exist within the document prior to dissemination or sharing by the MCAC.

k. Suspicious Activity Reporting (SAR) and Information Sharing Environment Suspicious Activity Reporting (ISE-SAR): The MCAC will apply the principals of this policy to tips and leads, suspicious activity report (SAR), and Information Sharing Environment SAR (ISE-SAR) information as defined by the DOJ Nationwide SAR Initiative (NSI) Program Management Office (PMO), to include the provisions for receipt, processing, storage, and dissemination of SAR and ISE-SAR information. In addition, prior to allowing access to or disseminating SAR and ISE-SAR information, MCAC personnel will ensure 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 a screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the information have been unsuccessful. MCAC will use the current standard reporting and cataloging

procedures for ISE-SAR information as set forth in the current version of the ISE-SAR Functional Standard (See n, below).

1) As with other information collected by the MCAC, all SAR and ISE-SAR information will be evaluated by an MCAC staff member to ensure the information is legally gathered and, when applicable, have a potential terrorism nexus. The MCAC will ensure that both law enforcement officers and MCAC personnel evaluating SAR and ISE-SAR information are trained in recognizing behavior consistent with criminal activity related to terrorism.

2) The ISE-SAR evaluation process will ensure, to the greatest degree possible, only information relating to individual involvement in criminal activity consistent with involvement in terrorism is documented via the ISE-SAR process and shared in the ISE. Information on protected activities as defined in section 6 (a) of this document, titled Seeking and Retaining Information, shall not be gathered, documented, processed, or shared via the ISE-SAR process unless relevant to the criminal activity or the identification of a terrorism subject.

3) SAR and ISE-SAR information will be stored 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.

4) 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).

5) 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.

6) Retain information for one year in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.

7) Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR (including ISE-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.

l. Sharing Of Information With Other Justice System Partners: Access to information gathered or retained by the MCAC will only be provided to persons within the MCAC or within other criminal justice, public safety, or regulatory agencies who are authorized access and only for legitimate law enforcement, public protection, prosecution, or other justice purposes, and only for the performance of official duties in accordance with applicable laws and procedures. Agencies receiving information from the MCAC may not distribute the information without the express consent of the MCAC or the agency originating the information. In accordance with established MCAC Standard Operating Procedures, an audit trail will be kept of access by or dissemination of information to such persons.

m. Distribution of Information Originating with Law Enforcement Partners: With documents or reports originating outside the center, MCAC personnel will make every attempt to ensure the privacy guidelines outlined in this policy are recognized and followed by the originating agency. If any information within these documents or reports is found to be in violation of this privacy policy, the information will not be distributed by the MCAC, and the originating agency will be notified of the MCAC's decision, with a detailed explanation, to include identification of errors or concerns. All requests for dissemination will be cataloged, with all request documentation (memorandum, e-mails, etc.) stored by the most efficient and non-obtrusive means available.

n. Sharing of Suspicious Activity Reporting Information: The MCAC will use the current version of the ISE-SAR Functional Standard issued by the Program Manager for the ISE for its ISE-SAR process, including the use of standard reporting format, commonly accepted data collection codes, and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism. The MCAC 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. In addition, the MCAC 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, which will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

o. Sharing of Information With Those Responsible For Public Protection, Safety, Or Health: Information gathered or retained by the MCAC may be disseminated to non-criminal justice public or private entities only for public protection, critical infrastructure protection, safety, or public health purposes and only in the performance of their official duties in accordance with applicable law and procedures. In accordance with established MCAC Standard Operating Procedures, an audit trail will be kept of access by or dissemination of information to such entities.

p. Disclosure of Information to the Public: Information gathered and retained by the MCAC will be disclosed to an individual member of the public only if the information as provided for in applicable law is defined to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. The MCAC will not confirm the existence or nonexistence of any information to any person or organization that would not be eligible to receive the information itself. In accordance with the MCAC Information Collection, Analysis, Dissemination, Retention and Destruction Policy, an audit trail will be kept of all public disclosure requests and their disposition.

q. Disclosure of Information for a Specific Purpose: Information gathered or collected and records retained by the MCAC 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 for a minimum of five years by the Center; the nature of the information requested, accessed, or received in response to the request, and the specific purpose will be maintained by the Center.

r. Non-Disclosure of Certain Information: The following are categories of records that will generally not be provided to the public pursuant to the Freedom of Information Act (5 U.S.C. § 552 (b))or other applicable laws, rules, or regulations:

1) Records required to remain confidential by law [5 U.S.C. § 552 (b)(3)];

2) Information that meets the definition of "classified information" as defined in the National Security Act, Public Law 235, Section 606 [5 U.S.C. § 552 (b)(1)];

3) Investigatory records compiled for law enforcement purposes that are legally exempted from disclosure requirements [5 U.S.C. § 552 (b)(7)(A)-(E)];

4) Could reasonably be expected to endanger the life or physical safety of any individual [5 U.S.C. § 552 (b)(7)(F)];

5) Information categorized as Protected Critical Infrastructure Information [6 C.F.R. § 29.8]

6) Protected federal, state, and local records, which may include records originated and controlled by another agency that cannot, under applicable state and federal laws, be shared without permission;

s. Redress: Records housed by the MCAC concerning an individual will be provided, upon review of the request by the MCAC Legal Counsel, to that individual upon proper verification of their identity, unless production or acknowledgement of the existence of such information is exempt under the Freedom of Information Act (5 U.S.C. § 552) or other existing statute or regulation, or the information is in a criminal intelligence information system subject to 28 CFR Part 23 (See 28 CFR §23.20(e)).

If the requested information does not reside or originate within the Center, the requestor will be referred to the originating agency in a manner that neither confirms nor denies the existence of the information. If a referral is made by the MCAC, the originating agency will notify the agency's listed point of contact.

t. Corrections: If a request is made by an individual or designee for correction of information originating within the MCAC that has been disclosed, the requestor will be informed of the procedure for requesting and considering required corrections, including appeal rights if requests are denied in whole or in part. The request will be reviewed and the requestor will be informed of the MCAC's decision, in writing, within 60 days of receipt of the request by MCAC, as specified in the U.S. Department of Justices Information Quality Guidelines. A record will be kept of all requests for corrections and the resulting action, if any.

u. Appeals: If access to information or a correction request for disclosed information originating within the MCAC is denied, the requestor will be provided, in writing, a reason for the denial. The individual will also be informed of the procedure for appeal when the center has cited an exemption for the type of information requested or when a correction request is either denied or not made to the satisfaction of the individual to whom the information relates.

v. Complaints: In the event the MCAC receives a complaint with regard to the accuracy or completeness of terrorism-related information held by the center, as it pertains to ISE-SAR, or other information that:

1) Is exempt from disclosure

a. Has been or may be shared through the Information Sharing Environment and allegedly resulted in demonstrable harm to the complainant;,

The MCAC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the MCAC Privacy Officer at the following e-mail address: mdwatch@leo.gov. The MCAC Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm nor deny the existence of the information unless otherwise dictated by law.

If the information did not originate within the MCAC, the Privacy Officer will notify the originating agency point of contact of the complaint either in writing or electronically within ten days, and upon request, assist the agency in correcting any information discrepancies as they relate to the complaint. All information relating to the complaint that is held by the MCAC will be reviewed within thirty days of receipt of the complaint, and corrected or purged if found to be inaccurate or incomplete, to include incorrectly merged records, or to be out of date. If there is no resolution within thirty days, the MCAC will not further share the information, if already shared, until corrective action is taken. The MCAC will record all complaints and resulting actions taken in response to them. To delineate protected information shared through the ISE from other data, MCAC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

w. Information Retention and Destruction: Information will be reviewed for purging in accordance with 28 CFR 23 and the MCAC Information Collection, Analysis, Dissemination, Retention and Destruction Policy. Criminal intelligence information, as defined in 28 CFR 23.3(b) is subject to annual review and will be purged after five years, unless the information is updated within that time period. (28 CFR 23.20(h)) When any other information is determined to have no further legitimate value, or meets the criteria for removal under the MCAC Information Collection, Analysis, Dissemination, Retention and Destruction Policy, it will be purged, destroyed, deleted, or returned to the submitting source as required. Notification of the proposed destruction or return of records may or may not be provided to the originating agency depending on the relevance of the information and any agreement with the originating agency. In accordance with the MCAC Information Collection, Analysis, Dissemination, Retention and Destruction Policy, a record of information to be reviewed for retention will be maintained by the MCAC and notice will not be provided to the submitter. A non-searchable record of purged or returned information will be maintained by the MCAC Privacy Officer for a period of one year. No approval will be required from the originating agency before information held by MCAC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

x. Unauthorized Release of Information or Breach of Data Systems; In the event information is released to the public without authorization, or the MCAC's data systems are breached, the MCAC will notify all affected individuals to whom it is determined may suffer physical, reputational, or financial harm as a result. The notice will be made promptly and without unreasonable delay following the discovery of an unauthorized release or breach, consistent with the legitimate needs of law enforcement to investigate the incident, determine the scope of the incident, and take measures to reasonably restore the integrity of the affected areas or systems. In addition, for information that does not originate in the MCAC, the originating agency will be immediately notified and informed of the nature and scope of the incident.

y. Information System Transparency: This policy will be made available to the public upon request and will be posted on the MCAC internet web at http://www.mcac-md.gov/. The Privacy Officer, established in Section 5. g. is responsible for receiving and responding to written inquiries and complaints about privacy rights, civil rights, and civil liberties protections in the information systems. The MCAC Privacy Officer can be contacted at mdwatch@leo.gov. .

z. Reporting Violations: MCAC staff will promptly report any and all violations of this policy to the MCAC Privacy Officer.

aa. Enforcement: If, after a thorough review, any MCAC employee, contractor, or participating agency/member is found to be in violation of this policy as it pertains to the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the MCAC will:

1) Immediately suspend access to MCAC and partner agency information systems by the person, persons, agency, or agencies involved in the violation.

2) If an individual is an MCAC employee or contractor, he or she will be referred to the Director for disciplinary action, up to and including termination of employment with the MCAC.

3) If an individual is detailed to the MCAC, or a member of a participating agency, he or she will be denied access to the MCAC and referred to their parent agency, with a complete report of the MCAC's findings as it relates to the violation and the MCAC's formal request for the initiation of disciplinary inquiries.

4) If appropriate, refer the violation to the appropriate law enforcement authority to initiate a criminal investigation.

5) The MCAC 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.

bb. Training: The following applies to training requirements for the protection of privacy, civil rights, and civil liberties in regard to the MCAC:

1) The MCAC will require the following individuals, upon assignment, to participate in training programs regarding implementation of and adherence to this policy:

a. All personnel assigned to the MCAC and Maryland Regional Information Centers;

b. Personnel providing information technology services to the MCAC;

c. Members of other agencies (employees or contractors) providing services to the MCAC; and

d. Any other personnel having access to information originating within the MCAC.

2) The training will be conducted annually and will cover:

a. The purpose of this policy;

b. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the MCAC;

c. Originating and participating agency responsibilities and obligations under applicable law and policy;

d. How to implement the policy;

e. The impact of improper activities associated with violations of this policy within and outside the MCAC;

f. Mechanisms for reporting violations of this policy; and

g. The nature and possible penalties for violations of this policy, including transfer, dismissal, civil and/or criminal liability, if any.

3) The MCAC 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 ISE.

cc. The Constitutional Protections Advisory Board:

1) The ATAC Executive Committee has established an independent MCAC Constitutional Protections Advisory Board (CPAB) to advise the Executive Committee and the Director of the MCAC on privacy rights, civil rights, and civil liberties policies and procedures regarding MCAC information acquisition, dissemination, and retention practices. The CPAB is comprised of three members not actively associated with or employed by any MCAC participating agency. The members are individuals with well established credentials in the fields of criminal justice and/or the law who have demonstrated unquestioned integrity and knowledge in the past practice of their professions. This policy will be reviewed and approved by the CPAB prior to submission to the ATAC.

2) The CPAB will at least annually review and recommend to the ATAC Executive Committee updates or changes to the MCAC's policy and procedure for protecting privacy rights, civil rights, and civil liberties in response to changes in applicable law, or as otherwise necessary.

3) The CPAB will review the results of Privacy Protection Policy compliance audits and necessary corrective actions taken, and advise the ATAC Executive Committee on any further corrective actions they may recommend.

4) The CPAB will conduct an independent inquiry into complaints alleging violation of the Privacy Rights Policy and will advise the ATAC Executive Committee of their findings and any recommended corrective action, if appropriate.

Appendix A

Definitions

The following is a list of primary terms and definitions used either in this policy, or that apply to the principals addressed within.

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.

ATAC—(Anti-Terrorism Advisory Council) An umbrella organization of local, state and federal agencies, as well as representatives from the private sector, that coordinates activities, develops policy, and implements strategic plans to combat terrorism in the State of Maryland.

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.

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

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 Maryland Coordination and Analysis Center (MCAC) and all participating federal, state, and local agencies and contractors assigned to the MCAC.

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 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.

Complaint- For the purpose of this policy, a complaint is a formal grievance or request for correction pertaining to information held by the Center.

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.

CPAB— The Constitutional Protections Advisory Board.

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— Criminal Intelligence is data that has been evaluated (analyzed) to determine that it:

A. is relevant to the identification of, and the criminal activity engaged in by, an individual or organization that is reasonably suspected of involvement in criminal activity; and
B. meets criminal intelligence system submission criteria as established in 28 CFR Part 23.

Further, criminal intelligence is information that is developed from data gathered by investigators and analysts. Criminal intelligence, because it has undergone some form of evaluation or analysis, indicates to law enforcement that the subject is likely to be involved in some definable criminal activity. It is more than separate pieces of information that by themselves mean nothing but, collectively, show an investigator or analyst an indication of the subject's criminal involvement.

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 to 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 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 USC § 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 an 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 policy is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the policy.

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.

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, as established by the Nationwide SAR Initiative (NSI) Program Management Office (PMO), 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 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 ruling, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information (as it pertains to terrorism)—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.

Law Enforcement Information (general) – Information that is related to a law enforcement mission.

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.

MCAC—The Maryland Coordination and Analysis Center (see Center).

Metadata—In its simplest form, metadata is information (data) about collected information, more specifically information about a particular aspect of that 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— Requested information which is pertinent and necessary to the requesting agency in initiating, furthering, or completing an investigation.

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, sending a message, or accessing data.

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. 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 may 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, as it relates to the Center, 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 also 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 Maryland constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23,; and applicable state , local and tribal laws and ordinances . Protections 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 or regulation authorizing access to the Center's information.

- Media organizations.

Public does not include:

- Employees or contractors of the Center or any participating agency.

- People or entities, private or governmental, who assist the Center in its operation.

- Public agencies whose authority to access information gathered and retained by the Center is authorized by law or regulation.

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. (See Complaints)

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, organization, or person 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, lawful, public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy may be the basis for a lawsuit for damages against the person or entity allegedly 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 overall electronic systems.

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, but are not limited to, surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, 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 and/or unevaluated 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 reports (SIR), suspicious activity reports (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tips and leads data. Tips and leads information does not include incidents without 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 when tied to other potentially related information that would otherwise seem disparate or unrelated.

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

Applicable Law

The following is a partial list of laws and regulations that may apply to this policy or to the general protection of privacy, civil right and civil liberties.

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

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat. 272