PRIVACY POLICY

A. PURPOSE

The Michigan Department of State Police (MSP) has primary responsibility of the Michigan Intelligence Operations Center (***MIOC***), for the overall operation of the ***MIOC***, its justice systems, operations, information collection and retention procedures, coordination of personnel, and the enforcement of the policy.

The purpose of the privacy, civil rights, and civil liberties policy is to promote ***MIOC*** and user conduct that complies with the federal, state, local, and tribal laws and assists the ***MIOC*** and its users in

- increasing public safety and improving national security;
- minimizing the threat and risk of injury to individuals;
- minimizing the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health;
- minimizing the threat and risk of damage to real or personal property;
- protecting individual privacy, civil rights, civil liberties, and other protected interests;
- protecting the integrity of the criminal investigatory, intelligence, and justice system processes and information;
- minimizing reluctance of individuals or groups to use or cooperate with the criminal justice system;
- supporting the role of the criminal justice system in society;
- promoting governmental legitimacy and accountability;
- not unduly burdening the ongoing business of the criminal justice system; and
- making the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legal Compliance with Laws Regarding Privacy, Civil Rights, and Civil Liberties

- Executive Order 2007-47 and Executive Order 2009-30: The creation of the Advisory Board for the ***MIOC*** for Homeland Security.

The ***MIOC***, after consultation with the Advisory Board, shall develop and publish a privacy policy for information and intelligence in the possession of the ***MIOC*** that is designed to protect the political and civil rights of Michigan residents, other individuals, and organizations consistent with applicable state and federal law, including, but not limited to, laws and regulations relating to privacy and public access to government information. The privacy policy shall preserve the integrity and effectiveness of law enforcement responsibilities and functions while also ensuring Michigan residents and other persons are not subject to the inappropriate use or release of protected information.

All ***MIOC*** personnel, personnel from fusion center nodes, participating agency personnel, personnel providing information technology services to the agency, private contractors, and authorized users will comply with the ***MIOC's*** privacy policy concerning the information the ***MIOC*** collects, receives, maintains, archives, accesses, or discloses to ***MIOC*** personnel, government agencies (including Information Sharing Environment (ISE) participating agencies) and participating justice and public safety agencies, as well as private contractors and the general public.

The ***MIOC***, all participating ***MIOC*** personnel, personnel providing information technology services to the ***MIOC***, private contractors, and users will comply with this policy and all applicable laws thus, protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

The ***MIOC*** will provide a printed copy of this policy to all personnel who are assigned to the ***MIOC*** and have direct access to ***MIOC*** information and will require both a written acknowledgement of receipt of this policy and a written agreement (Non-Disclosure Agreement) to comply with this policy and the provisions it contains.

The ***MIOC*** has adopted internal operating policies and procedures that apply to all personnel, including participating agency personnel, personnel providing information technology services to the agency, private contractors, agencies that originate information, and other authorized users. The ***MIOC*** is in compliance with applicable laws protecting privacy, civil rights and civil liberties, including, but not limited to:

- **U.S. Constitution, 1st, 2nd, 4th, 5th, 6th, 8th and 14th Amendments**
  http://topics.law.cornell.edu/constitution

- **Michigan Constitution, Article I, Sections 1 through 23**
  http://www.legislature.mi.gov/(S(vw4qql55dlqellygwpc3gs55))/mileg.aspx?page=getObject&objectName=mcl-Constitution

- **Interstate Law Enforcement Intelligence Organizations Act, Public Act 201 of 1980, MCL 752.1 through 752.6**
  http://www.legislature.mi.gov/(S(mx52as55nnceadnubsd2rxup))/mileg.aspx?page=getObject&objectName=mcl-Act-201-of-1980&highlight=752.1

- **C.J.I.S. Policy Council Act, Public Act 163 of 1974, MCL 28.211 through 28.216**
  http://legislature.mi.gov/doc.aspx?mcl-act-163-of-1974

- **Social Security Number Privacy Act, Public Act 454 of 2004, MCL 445.81 through 445.87**
  http://www.legislature.mi.gov/(S(nma4cgr5wgrix0q4tpue24rg))/mileg.aspx?page=getobject&objectname=mcl-Act-454-of-2004&query=on&highlight=445.81

- **Bureau of Justice Assistance – Criminal Intelligence Systems Operating Policies (28 CFR Part 23)**
  http://www.iir.com/28cfr/guideline1.htm

- **Protected Critical Infrastructure Information (PCII), 6 CFR Part 29**
  http://law.justia.com/us/cfr/title06/6-1.0.1.1.9.html
  PCIIMS Training Link: https://pciims.dhs.gov/pciims/index.aspx

- **National Security Classified Documents Executive Order No 13526, December 29, 2009**
  http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information

- **National Crime Prevention and Privacy Compact**, 42 U.S.C. § 14616
  http://law.justia.com/us/codes/title42/42usc14616.html

- **Privacy Act of 1974**, 5 U.S.C. § 552a
  http://www.justice.gov/opcl/privstat.htm

C. GOVERNANCE and OVERSIGHT

Primary responsibility for the operation of the ***MIOC***, its systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis destruction, sharing, or disclosure of the information; and the enforcement of this policy is assigned to the Director of ***MIOC*** within the MSP. The ***MIOC*** is guided by an agency-designated privacy committee that liaises

with community privacy advocacy groups to ensure that privacy and civil rights are protected within the provisions of this policy and within the ***MIOC's*** information collection, retention, and dissemination processes and procedures.

The ***MIOC*** privacy committee is guided by a trained privacy officer who is appointed by the Director of the ***MIOC*** who will select the most qualified individual to serve in this position. The ***MIOC*** Privacy Officer receives reports regarding alleged errors and violations of the provision of this policy, receives and coordinates complaint resolution under the ***MIOC's*** redress policy, and is the liaison to the ISE, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies. The ***MIOC's*** Privacy Officer ensures that enforcement procedures and sanctions outlined in Section N.3, Enforcement, are adequate and enforced.

The contact information for the ***MIOC*** Privacy Officer is as follows:

- ***MIOC*** Privacy Officer
  Michigan State Police
  333 S. Grand Avenue
  P.O. Box 30634
  Lansing, MI 48909-0634

  MSP-MIOC-PrivacyOfficer@michigan.gov

D. DEFINITIONS

Refer to Appendix A, Terms and Definitions.

E. INFORMATION

The ***MIOC*** will seek or retain information that

- is based on criminal predicate or possible threat to public safety; or
- is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity; or
- is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting criminal justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
- is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); and
- the source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
- was collected lawfully.

The ***MIOC*** may retain information that is based on a level of suspicion that is less than reasonable suspicion such as tips and leads or official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity (suspicious activity reporting (SAR)).

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

The ***MIOC*** will ensure standardized labeling is applied to center and agency-originated information (or will ensure that the originating agency has applied labels) to indicate to the accessing authorized user that

- the information pertains to all individuals and organizations (as expressly provided herein); and
- the information is subject to Michigan and Federal laws restricting access, use, or disclosure.

The ***MIOC*** personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency assigns categories to the information) to reflect the assessment, such as

- whether the information consists of tips and leads data, suspicious activity reports, criminal history or intelligence information, case records, conditions of supervision, or case progress, etc.;
- the nature of the source as it affects veracity (e.g. anonymous tip, trained interviewer or investigator, public record, private sector);
- the reliability of the source (e.g. confirmed, probable, doubtful, cannot be judged).
- the validity of the content (e.g. confirmed, probable, doubtful, cannot be judged).

At the time the decision is made 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 individual's right of privacy, civil rights, and civil liberties; and
- provide legally required protection based on the individual's status as a child, sexual abuse victim, crime victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

Existing information will be re-evaluated whenever

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

MIOC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips, leads, and SAR information.

The nature of the information may indicate an imminent or developing threat to the safety of persons and property and may require immediate dissemination without the opportunity to assess or validate this information. Information released under these circumstances must be identified as being based on initial reporting or developing information.

Except as provided in the above paragraph, ***MIOC*** 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 that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information;

- allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, “need-to-know” and “right-to-know” access or dissemination for personally identifiable information);

- regularly provide access to or disseminate the information in response to an inter-agency inquiry for law enforcement, homeland security, 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 90 days in order to work an un-validated tip, lead, or SAR information to determine its credibility and value, assign a “disposition” label (i.e., undetermined, unresolved, cleared or unfounded, or under active investigation) so that a subsequent authorized user knows that status and purpose for the retention and will retain the information based on the retention period associated with the disposition label; and

- adhere to and follow the ***MIOC’s*** physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SAR information will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.

The ***MIOC*** 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 constitutional rights, including personal privacy and other civil liberties and civil rights.

The ***MIOC*** will identify and review protected information that is originated by the ***MIOC*** prior to sharing that information through the ISE. Further, the ***MIOC*** 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. The ***MIOC*** requires certain, basic descriptive information to be entered and

electronically associated with the data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure. The types of information should include;

- the name of the originating department, component, and subcomponent;
- the name of the agency'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.

The ***MIOC*** 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 ***MIOC*** will keep a record of the source of all information retained by the agency.

F. Acquiring and Receiving Information (Refer to Appendix B)

Information gathering (acquisition and access) and investigative techniques used by the ***MIOC*** and information-originating agencies are in compliance with and will adhere to applicable regulations and guidelines, including, but not limited to,

- 28 CFR Part 23 regarding criminal intelligence information;
- Organization for Economic Co-operation and Development's (OECD) Fair Information Practices (under certain circumstances, there may be exceptions to the Fair Information Practices, based, for example, on authorities paralleling those provided in the Federal Privacy Act; state, local, and tribal laws; or ***MIOC*** policy);
- applicable criminal intelligence information guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP); and
- applicable constitutional provisions as described in Section B of this policy and the applicable administrative rules as well as any other regulations that apply to multi-jurisdictional criminal intelligence information databases.

The ***MIOC's*** SAR process provides for human review and vetting to ensure that information is both gathered legally and, where applicable, determined to have a potential terrorism or criminal nexus. Law enforcement officers and ***MIOC*** staff will be trained to recognize those actions and incidents that are indicative of criminal activity related to terrorism. The ***MIOC's*** SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights and civil liberties will not be intentionally or inadvertently gathered, documented, processed, or shared.

Information gathering and investigative techniques used by the ***MIOC*** shall be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain. External agencies that access and share information with the ***MIOC*** are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws. The ***MIOC*** 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 collection practices.

The ***MIOC*** will not directly or indirectly receive, seek, accept, or retain information from an individual or information provider that is legally prohibited from obtaining or disclosing the information**.** The ***MIOC*** may receive information from an individual or nongovernmental entity that may receive a fee or benefit for providing the information as provided by law, ***MIOC*** and MSP policy.

G. INFORMATION QUALITY ASSURANCE

The ***MIOC*** will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information, 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 has been met. At the time of retention in the system, the information will be labeled regarding this level of quality (accurate, complete, current, verifiable and reliable). The ***MIOC*** 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 labeling of retained information will be re-evaluated when new information is gathered that has impact on the confidence (validity and reliability) in previously retained information.

The ***MIOC*** will conduct periodic data quality reviews of information it originates and will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the agency (***MIOC***) learns that the information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the agency; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer. Originating agencies external to the ***MIOC*** are responsible for the quality and accuracy of the data accessed by or provided to the ***MIOC***. The ***MIOC*** will advise the appropriate contact person in the originating agency, **in writing,** if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

The ***MIOC*** will use written or documented electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the ***MIOC*** (i.e., when information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected).

H. COLLATION and ANALYSIS

Information acquired or received by the ***MIOC*** (as identified in Section E) or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly. Information acquired or received by the ***MIOC*** or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to

- further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by the ***MIOC***; and
- provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or are engaging in criminal activities (including terrorism).

I. MERGING RECORDS

The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye or hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number, or other biometrics, such as DNA,

retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

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

J. SHARING and DISCLOSURE

Credentialed, role-based access criteria will be used by the ***MIOC***, as appropriate, to control

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

The ***MIOC*** adheres to national standards for the ISE-SAR process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for SAR potentially related to terrorism.

Access to or disclosure of records retained by the ***MIOC*** will be provided to persons within the center or in other governmental agencies for legitimate law enforcement, public protection, public prosecution, public health, or criminal justice purposes and in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the ***MIOC*** and the nature of the information accessed will be kept by the ***MIOC***.

Agencies external to the ***MIOC*** may not disseminate information accessed, received, or disseminated from the center without documented approval from the center or other originator of the information.

Information gathered and records retained by the ***MIOC*** may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those users and purposes specified in the law. An audit trail SHALL be kept for a minimum of five (5) years of requests for access to information for specific purposes including what information is disseminated to each person in response to the request.

Information gathered and records retained by the ***MIOC*** may be accessed or disclosed to members of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the agency's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the ***MIOC*** for the type of information or when there is a legitimate need. An audit trail SHALL be kept of all requests including what information is disclosed to a member of the public.

Information gathered and records retained by the ***MIOC*** **SHALL NOT** be:

- sold, published, exchanged, accessed or disclosed for commercial or personal purposes;
- disclosed or published without prior notice to the originating agency that such information is subject to re-disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency; or
- disseminated to persons not authorized to access or use the information.

There are several categories of records that will not ordinarily be provided to the public (refer to Appendix B of this policy for detailed legal citations) and are exempt from disclosure requirements including the following

- Records required to be kept confidential by law MCL 15.243 (13) (d).
- Investigatory records of law enforcement agencies. However, certain records must be made available for inspection and copying under Michigan Law, i.e., Michigan Compiled Laws (MCL) 15.231, et seq. commonly referred to as "Freedom of Information Act (FOIA)", Public Act 442 of 1976, as amended. These Freedom of Information (FOI) requests will be addressed with coordination between the ***MIOC*** Privacy Officer and the Michigan State Police, Reporting and Analysis Division, Freedom of Information Unit.
- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempt from disclosure under MCL 15.231 et seq. These FOI requests will be addressed with coordination between the ***MIOC*** Privacy Officer and the Michigan State Police, Reporting and Analysis Division, Freedom of Information Unit. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism, an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission MCL 15.243 (13) (d).

The ***MIOC*** shall not confirm the existence or non-existence of information to any person or agency that would not be eligible to receive the information itself except as otherwise required by law.

K. REDRESS

K.1. Disclosure

Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in K.2 (below), an individual is entitled to know the existence of, and review the information about, him or her that has been gathered and retained by the ***MIOC***. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The ***MIOC's*** response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and including what information is disclosed to an individual.

The existence, content, investigative methods, and source of the information will NOT be made available to an individual when

- disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (MCL 15.243(1)(b);
- disclosure would endanger the health or safety of an individual, organization, or community; (MCL 15.243, sec 13);
- the information is in a criminal intelligence system; (MCL 15.243;
- the information source does not reside with the ***MIOC*** (when information is not disclosed because it did not originate with the ***MIOC***, the request

will be referred to the originating agency, if appropriate) (Michigan Freedom of Information Act, Act 442 of 1976;

- the ***MIOC*** did not originate or does not have a right to disclose the information; (Michigan Freedom of Information Act, Act 442 of 1976;
- other **authorized** basis for denial under MCL 15.243; or
- disclosure would violate state or federal law.

K.2. Complaints and Corrections

If an individual objects to the accuracy or completeness of information about him or her originating with the agency that has been disclosed, the ***MIOC*** will inform the individual of the procedure for requesting corrections.

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 the ***MIOC*** and
  (2) allegedly has resulted in demonstrable harm to the complainant.

The individual shall be informed of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the ***MIOC's*** Privacy Officer. Please refer to Section C of this policy for the Privacy Officer's contact information.

The Privacy Officer or ***MIOC*** Commander will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the ***MIOC***, the Privacy Officer or ***MIOC*** Commander will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data or record deficiencies, purge the information, or verify that the record is accurate.

All information held by the ***MIOC*** that is the subject of a complaint will be reviewed within 30 days and confirmed, corrected, or purged if determined to be inaccurate or incomplete, including incorrectly merged information or information that is out of date. If there is no resolution within 30 days, the ***MIOC*** will not share the information until such time as the complaint has been resolved. A record will be kept by the ***MIOC*** of all complaints and the resulting action taken in response to the complaint.

A record will be kept of all complaints and requests for corrections and the resulting actions, if any.

To delineate protected information shared through the ISE from other data, the ***MIOC*** maintains records of the source or originating agencies to which the ***MIOC*** has access, as well as audit logs, and employs system mechanisms whereby the source (or originating agency, including source or originating agencies) is identified within the information.

The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the ***MIOC***. The individual will also be informed of the procedure for appeal when the ***MIOC*** has declined to correct the challenged information to the satisfaction of the individual to whom the information relates.

K.3 Appeal

Upon notice of denial of a request for the release of information or complaint made under section K or subsection K.2 of this policy, the requester may file a request for information under the Michigan Freedom of Information Act, Public Act, 442 of 1976. If the Freedom of Information request is denied, the requester shall follow the process for appealing this decision as required by MCL 15.240.

L. SECURITY SAFEGUARDS

The ***MIOC*** Director will designate an individual who will be properly trained and will serve as the ***MIOC's*** Security Officer.

The ***MIOC*** will operate in a secure facility protecting the facility from external intrusion. The ***MIOC*** will utilize secure internal and external safeguards against network intrusions. Access to ***MIOC*** databases from outside the facility will be allowed only over secure networks.

The ***MIOC*** will secure tips, leads, and SAR information in a separate repository system that is the same as, or similar to, the system that secures data rising to the level of reasonable suspicion. In order to prevent public records disclosure, risk and vulnerability assessments shall not be stored with publicly available data. The ***MIOC*** will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such action.

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

Queries made to the ***MIOC*** data applications will be logged into the data system identifying the user initiating the query. The ***MIOC*** will utilize watch logs to maintain audit trails of requested and disseminated information.

The ***MIOC*** will notify an individual whose personal information or sensitive personally identifiable information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputation, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release, or the ***MIOC*** will follow the guidance set forth in the Identity Theft Protection Act, MCL 445.63, et seq.

M. INFORMATION RETENTION and DESTRUCTION

All applicable criminal intelligence information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23.

SAR data will be maintained and purged as provided by this policy, ***MIOC*** retention policy, or as required by law.

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

When information has no further value or meets the criteria for removal according to the ***MIOC's*** retention and destruction policy or according to applicable law, it will be purged, destroyed, deleted or returned to the submitting (originating) agency.

The procedure contained in the ***MIOC*** Policy and Procedures Manual will be followed for notification to appropriate parties including the originating agency, before information is deleted or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.. The notification of proposed destruction or return of records may be provided to the source agency, depending on the relevance of the information and any agreement with the providing agency. A record of information to be reviewed for retention will be maintained by the ***MIOC***, and, for appropriate systems, notice will be given to the submitter at least 30 days prior to the required review and validation or purge date.

N. ACCOUNTABILITY and ENFORCEMENT

N.1. Information System Transparency

The ***MIOC*** will be open with the public in regard to information and intelligence collection practices. The ***MIOC's*** privacy policy will be provided to the public for review, made available upon request, and posted on the ***MIOC's*** Web site at http://www.michigan.gov/MIOC.

The ***MIOC's*** Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information systems maintained or accessed by the ***MIOC***. Please refer to Section C of this policy for the Privacy Officer's contact information.

N.2. Accountability

The audit log of queries made to the ***MIOC's*** Criminal Intelligence Information System will identify the user initiating the query. The ***MIOC*** 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 what information is disseminated to each person in response to the request.

The ***MIOC*** will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with provisions of this policy and applicable law. This will include logging access of these systems and periodic auditing of these systems so as to not establish a pattern of the audits. These audits will be mandated at least quarterly, and a record of the audits will be maintained by the Director of the ***MIOC***.

The ***MIOC*** will annually conduct an audit and inspection of the information contained in its criminal intelligence system. The audit will be conducted by an independent entity designated by the Director of the MSP. This independent entity has the option of conducting a random audit, without announcement, at any time and without prior notice to the ***MIOC***. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy or the ***MIOC's*** criminal intelligence system.

The ***MIOC's*** privacy committee, guided by an appointed and trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained within 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 ***MIOC's*** personnel or other authorized users shall report violations or suspected violations of ***MIOC*** policies relating to protected information to the ***MIOC's*** Privacy Officer.

N.3 Enforcement

If ***MIOC*** personnel, a participating agency, or any authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, access or disclosure of information, the Director or the ***MIOC*** will

- suspend or discontinue access to information by the user;
- suspend, demote, transfer, or terminate the person, as permitted by applicable personnel policies;
- apply administrative actions or sanctions as provided by MSP rules and regulations or as provided in ***MIOC*** personnel policies;
- if the user is from an agency external to the MSP, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions;
- refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy; or
- brief the ***MIOC*** Advisory Board of any violations of this policy and actions taken.

The ***MIOC*** reserves the right to restrict the qualifications and number of personnel having access to ***MIOC*** information and to deny access to any participating agency or individual user who fails to comply with the applicable restrictions and limitations of the ***MIOC's*** privacy policy.

O. TRAINING

The ***MIOC*** will require all of the following individuals to participate in training programs regarding implementation of, and adherence to, the privacy, civil rights, and civil liberties policy:

- all assigned personnel of the ***MIOC***;
- personnel providing information technology services to the ***MIOC***;
- staff in other public agencies or private contractors providing services to the agency; and
- users who are not employed by the MSP or a contractor.

The ***MIOC*** will provide special training to personnel authorized to share protected information through the ISE regarding the ***MIOC's*** requirements and policies for collection, use, access, and disclosure of protected information.

The ***MIOC's*** privacy policy training program will cover

- purposes of the privacy, civil rights, and civil liberties protection policy;
- substance and intent of the provision of the policy relating to the collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the ***MIOC***;
- how to implement the policy in the day-to-day work of the user, whether a paper or systems user;

- the impact of improper activities associated with the infractions within or through the agency;
- mechanisms for reporting violations of ***MIOC*** privacy-protection policies; and
- the nature and possible penalties for policy violations including, but not limited to, possible transfer, dismissal, criminal liability, and immunity, if any.
- originating and participating agency responsibilities and obligations under applicable law and policy.

Training programs developed or provided by the ***MIOC*** will be submitted to the ***MIOC*** Advisory Board for review.

P. POLICY ENFORCEMENT

Any individual who is deemed in violation of this policy may be subject to documentation in their annual performance appraisal &/or disciplinary action in accordance with civil service and department rules.

Q. REVISION RESPONSIBILITY

The responsibility for revision of this policy lies with the Section Manager, ***MIOC*** Training and Development Unit with the approval of the ***MIOC*** Commander.

This area is intentionally left blank

APPENDIX A
Terms and Definitions

The following is a list of primary terms and definitions used throughout this policy. These terms may also be useful in drafting the definitions section of the agency's privacy policy.

Access—Data access is being able to obtain (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 through which ISE participants obtain terrorism-related information including, but not limited to, homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

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

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

Agency—Agency refers to all jurisdictions at any level that access, contribute, and share information in the ***MIOC***.

Audit Trail—Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

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

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

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

Civil Liberties—Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights**—**the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action

and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions by government.

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

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

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

Criminal Intelligence Information or Data—Information deemed relevant to the identification of, and the criminal activity engaged in by, an individual who, or organization that is, reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information.

Criminal Predicate—Sufficient, articulable facts, along with rational inferences from those facts, to give employees working under the supervision of a law enforcement agency a basis to believe there is a reasonable possibility that a person is involved in criminal or terrorist activity.

Data—Inert symbols, signs, descriptions, or measures.

Data Breach— The unintentional release of secure information to an un-trusted environment. This may include incidents such as theft or loss of digital media, e.g., computer tapes, hard drives, or laptop computers containing media upon which information is stored unencrypted; posting such information on the Internet 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, as in unencrypted e-mail; or transfer of information to the information systems of a possible hostile agency or environment where it may be exposed to more intensive decryption techniques.

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

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

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organisation 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 trans-border exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are

1. Collection Limitation Principle,
2. Data Quality Principle,
3. Purpose Specification Principle,
4. Use Limitation Principle,
5. Security Safeguards Principle,
6. Openness Principle,
7. Individual Participation Principle, and
8. 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.

Fusion Center—A multi-agency organization to better enable information sharing between member agencies in support of investigations, homeland and national security, and reduce threats. A collaborative effort of two or more agencies that provides resources, expertise , and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorism activity. Note: the Department of Homeland Security has categorized fusion centers as *Primary Designated Fusion Centers* or as *Designated Fusion Centers.* To be designated into these categories, the following criteria must be met:

- **Primary Designated Fusion Center**
  - is designated by the Governor as the primary state center;
  - is responsible for passing relevant homeland security information received from the federal government to other centers in the state as well as to nonparticipating law enforcement agencies;
  - Agrees to follow the Fusion Center Guidelines and work toward attaining the Baseline Capabilities for fusion centers;
  - is managed and run by the state, or the state's designee, in which the center is located;
  - receives some level of federal support; and
  - comprises two or more state or local agencies.

- **Designated Fusion Center**
  - is managed and run by a nonfederal entity;
  - is located in an Urban Area Security Initiative city;
  - agrees to follow the Fusion Center Guidelines and work toward attaining the Baseline Capabilities for fusion centers;
  - receives some level of federal support;
  - comprises two or more state or local agencies; and
  - agrees to work in conjunction with the Primary Designated Fusion Center.

Fusion Center Nodes or Nodes—A fusion center or designated fusion center that participates, is interconnected, collaborates, and shares information with the Primary Designated Fusion Center.

General Information—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 or retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

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

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

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

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

Information Sharing Environment (ISE)—The terms "information sharing environment" and "ISE" mean an approach that facilitates the sharing of terrorism information. The ISE provides and facilitates the means for sharing all threats, all hazards information among all appropriate federal, state, local and tribal entities, and the private sector through the use of policy guidelines and technologies and shall ensure the protection of privacy and civil liberties.

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

Information Quality—Information quality refers to various aspects of the information including 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 or meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

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 multi-source information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

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

Label—An identifier displayed with or attached to a document, record, field or page providing a descriptive or identifying word or phrase as to the status, condition, classification or other important data concerning a data record, document, or other information.

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

Law Enforcement Information—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 or witness assistance.

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

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

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

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

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

Michigan Intelligence Operations Center (*MIOC*) —The primary designated fusion center serving the state of Michigan, established by Governor Jennifer Granholm via Executive Order 2007-47 on December 20, 2007.

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

Node—Refer to **"Fusion Center Node"**

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

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

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

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

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

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

- personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of

birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans);

- a unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number);
- descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records); and
- descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons—United States Intelligence Activities, Executive Order No. 12333, December 4, 1981 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

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

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

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

Private Partner —An individual, entity, or organization that participates and contributes to the intelligence cycle or the ISE.

Protected Information—Information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the United States Constitution and laws of the United States. While not within the definition established by the ISE Privacy Guidelines, protection may be extended to other individuals and organizations by internal federal agency policy or regulation.

For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order No. 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

For state, local, and tribal governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws, ordinances, and codes. Protection may

be extended to other individuals and organizations by fusion center or other state, local, or tribal agency policy or regulation.

Public—Public includes

- any person and any for-profit or nonprofit entity, organization, or association;
- any governmental entity for which there is no existing specific law authorizing access to the agency's/***MIOC's*** information;
- media organizations; and
- entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does **not** include

- employees of the agency;
- people or entities, private or governmental, who assist the agency (***MIOC***) in the operation of the justice information system; and
- public agencies whose authority to access information gathered and retained by the agency/***MIOC*** is specified in law.

Public Access—Public access relates to what information can be seen by the public, i.e. information whose availability is not subject to privacy interests or rights.

Reasonable Suspicion—Is a legal standard in United States law that a person has been, is, or is about to be engaged in criminal activity based on specific and articulable facts and inferences. It is the basis for an investigatory or "Terry Stop" by the police and requires less evidence than probable cause, the legal requirement for arrests and warrants. Reasonable suspicion is evaluated using the "reasonable person" or "reasonable officer" standard, in which a person in the same circumstances could reasonably believe a person has been, is, or is about to be engaged in criminal activity; such suspicion is not a mere hunch. Police may also, based solely on reasonable suspicion of a threat to safety, frisk a suspect for weapons, but not for contraband. A combination of particular facts, even if each is individually innocuous, can form the basis of reasonable suspicion.

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

Redress—Internal procedures to address complaints from persons regarding protected information about them that is under the agency's (***MIOC's***) control.

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

Retention—Refer to "**Storag**e"

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

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

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

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

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:

1. 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 meaning is probably more common in the IT industry than meaning 2.

2. 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, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Suspicious Activity—Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Report (SAR)—Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. 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 Intelligence Reform and Terrorism Prevention Act (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 IRTPA, as recently amended by the 9/11 Commission Act (being Pub. L. 110-53, August 3, 2007), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act(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 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 includes intelligence information. Weapons of Mass Destruction (WMD) information as a

fourth (third statutory) category of ISE information is not called for in Pub. L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not technically be cited or referenced as a fourth category of information in the ISE.

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

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

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

End of Terms and Definitions

This area is intentionally left blank

APPENDIX B

Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Excerpt from U.S. Department of Justice's (DOJ's)
Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, and tribal (SLT) agencies. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution but can (and many do) provide enhanced privacy and other civil liberties protections.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the ISE is explored in a key issues guidance paper titled Civil Rights and Civil Liberties Protection, which is available on the Program Manager (PM) for the Information Sharing Environment (PM-ISE) Web site at www.ise.gov.

Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Persons Act.

Federal laws, Executive Orders, regulations, and policies directly affect agencies'/***MIOC***s' privacy policies. While SLT agencies may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the information collection sharing context, compliance may be required indirectly by funding conditions (e.g., 28 CFR Parts 20, 22, and 23 or the Health Insurance Portability and Accountability Act [HIPAA]); operation of the Commerce Clause of the U.S. Constitution (e.g., Electronic Communications Privacy Act of 1986); or a binding agreement between a federal agency and an SLT agency (e.g., a memorandum of agreement or memorandum of understanding). Where relevant or possibly relevant, agencies/***MIOC***s are advised to list these laws, regulations, and policies, noting those that may potentially affect the sharing of information, including sharing terrorism-related information in the ISE.

The development of a privacy, civil rights, and civil liberties policy is primarily designed for agency/***MIOC*** personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the agency/***MIOC*** must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an agency/***MIOC*** privacy policy, staff and user accountability is greatly diminished, mistakes are made, privacy violations occur, and the public's (and other agencies') confidence in the ability of the agency/***MIOC*** to protect information and intelligence is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, information sharing is enhanced.

Below is a partial listing of federal laws that should be reviewed when developing a privacy policy for a justice information system. The list is arranged in alphabetical order by popular name.

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

Michigan Freedom of Information Act (FOIA), Public Act, 442 of 1976,

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, Pub. L. 108-458, 118 Stat. 3638 (Dec. 17, 2004), as amended by the 9/11 Commission Act.

National Child Protection Act of 1993, Pub. L. 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

Posse Comitatus Act 18 U.S.C. § 1385, Title 18, U.S. Code, Section 1385

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

U.S. Constitution, First, Fourth, and Sixth Amendments

USA PATRIOT Act, Public Law No. 107-56 (October 26, 2001), 115 Stat. 272