DSEMIIC

DETROIT & SOUTHEAST MI INFORMATION CENTER

PRIVACY POLICY

TABLE OF CONTENTS

A STATEMENT OF PURPOSE

The mission of the DSEMIIC (Detroit & Southeast MI Information Center) is to identify, monitor, analyze and disseminate information, using an all terrorism, all crimes, all hazards, risks-based approach, in support of law enforcement, public safety, and the private sector's efforts to prevent, protect, and prepare for threats to Southeast Michigan. To ensure the rights and privacy of citizens, Fair Information Practices will be followed.

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

- Increasing public safety and improve national security;
- Minimizing the threat and risk of injury of specific 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, criminal intelligence, and justice system processes and information;
- Minimizing reluctance of individuals or groups to use or cooperate with the justice system;
- Supporting the role of the justice system in society;
- Promoting governmental legitimacy and accountability;
- Not unduly burdening the ongoing business of the justice system; and
- Making the most effective use of public resources allocated to justice agencies.

B POLICY APPLICABILITY AND LEGAL COMPLIANCE

1. All DSEMIIC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, and all other authorized users will comply with DSEMIIC's privacy policy, to which they are legally bound, in order to protect privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing and disclosure of information, both within the center and participating justice and public safety agencies (including Information Sharing Environment [ISE] participating centers and agencies), as well as to private contractors, private entities, and the general public.

2. Definitions of primary terms used in this policy are set forth in Appendix A.

3. The contents of this privacy policy provide internal guidance to participating DSEMIIC personnel and are in compliance with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to, those listed in Appendix B. Nothing in the policy is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties.

4. The DSEMIIC will provide a printed copy of this policy to all center and non-center personnel who provide services. All participating agency personnel, personnel providing information technology services to the agency, private contractors, and all other authorized users will be required to provide a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

5. All DSEMIIC personnel, personnel providing information technology services to the agency, private contractors, and all other authorized users are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to those listed in Appendix B.

C GOVERNANCE AND OVERSIGHT

1. Primary responsibility for the operation of the DSEMIIC; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information and the enforcement of this policy is assigned to the Executive Director of the DSEMIIC.

2. The DSEMIIC Advisory Board will approve the DSEMIIC Privacy Policy and will coordinate with the center's Community Liaison to ensure that privacy, civil rights, and civil liberties are protected as provided in this policy and by the center's information gathering and collection, retention, and dissemination processes and procedures. The Advisory Board, guided by the center's Privacy Officer (L, L.2, 6), will annually review and update the policy in response to changes in law and implementation experience, including the results of audits and inspections.

3. The DSEMIIC Advisory Board is guided in privacy related issues by a trained Privacy Officer who is appointed by the Executive Director of the DSEMIIC. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, coordinates complaint resolution under the center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies. The Privacy Officer can be contacted at the following e-mail address: Fusion_Center@detroitmi.gov**.**

4. The DSEMIIC's Privacy Officer ensures that enforcement procedures and sanctions outlined in Section L.3 are adequate and enforced.

5. DSEMIIC employees, contract employees and persons on assignment to the DSEMIIC from other agencies are responsible for adhering to this policy. Failure to abide by this policy may result in disciplinary action up to and including dismissal.

D INFORMATION

1. The DSEMIIC will seek or retain only information that is:

   - Based on a possible threat to public safety or the enforcement of the criminal law, or
   - Relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
   - Collected by criminal justice agencies on specific individuals, consisting of official identifiable descriptions and notations of arrests, detentions, warrants, complaints, indictments, information, or other formal criminal charges and any disposition relating to these charges, including acquittal, sentencing, pre- or post conviction supervision, correctional supervision, and release, or
   - Where there is reasonable suspicion that a specific individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity, or
   - Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches); and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

   The DSEMIIC may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in Section D8.

2. The DSEMIIC 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 races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

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

   - The information is protected information, as defined by the center to include personal data on any individual (see Appendix A) and, to the extent expressly provided in this policy, includes organizational entities.

- The information is subject to local, state or federal law (see Appendix B), including 18 U.S.C. §2721 et seq., MCL 15.231 et seq., MCL §3.1051, MCL445.81, MCL §445.1711, and 500.501 and any other law restricting access, use, or disclosure.

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

   - Where the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.

   - The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).

   - The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).

   - The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. The DSEMIIC 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.

6. The DSEMIIC will identify and review protected information that is originated by the center prior to sharing that information through the Information Sharing Environment (ISE). Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

7. The DSEMIIC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:

   - The name of the originating center, department or agency, component, and subcomponent.

   - The name of the center's justice information system from which the information is disseminated.

   - The date the information was collected and, where feasible, the date its accuracy was last verified.

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

8. DSEMIIC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. The DSEMIIC personnel will:

    - Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The DSEMIIC will use a standard reporting format and data collection codes for SAR information.

    - Store the information using the same storage method used for data that rises to the level of reasonable suspicion and 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).

    - Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.

    - Retain information for up to 90 days to work a tip or lead or SAR information to determine its credibility and value, assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, or under active investigation) so that a subsequently 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.

    - Adhere to and follow the center’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.

9. The DSEMIIC 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 restriction on information sharing based on information sensitivity or classification.

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

E ACQUIRING AND RECEIVING INFORMATION

1. Information gathering and investigative techniques used by the DSEMIIC and information originating agencies will comply with all applicable state and federal laws in Appendix B. They will be no more intrusive or broad scale than is necessary in the particular circumstances to gather information it is authorized to seek or retain.

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

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

4. External agencies that access and share information with the DSEMIIC are governed by the laws and rules governing those individual agencies, as well as by applicable laws in Appendix B.

5. The DSEMIIC 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.

6. The DSEMIIC will not directly or indirectly receive, seek, accept, or retain information from:
   - An individual or nongovernmental entity who may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.; or
   - An individual or information provider that is legally prohibited from obtaining or disclosing the information

F CLASSIFICATION OF INFORMATION

1. At the time of retention in the system, the information will be categorized regarding its content validity, nature of the source, and source reliability.

- The labeling of retained information will be reevaluated when new Information is gathered that has an impact on the validity and reliability of retained information.

- Classification of information regarding limitations on access and disclosure at the time a decision is made to retain information, will be classified pursuant to the applicable limitations on access and sensitivity of disclosure in order to:

    a. Protect confidential sources and police undercover techniques and methods;

    b. Not interfere with or compromise pending criminal investigations;

    c. Protect an individual's right of privacy and civil rights; and

    d. Provide legally required protection based on the status of an individual as a victim or witness;

    e. Provide and ensure protection against unauthorized or prohibited disclosure.

2. The classification of existing information will be reevaluated whenever:

    - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or

    - There is a change in the use of the information affecting access or disclosure limitations.

G INFORMATION QUALITY ASSURANCE

1. The DSEMIIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; and 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 (as referenced in Section I, Merging of Information From Different Sources) has been met.

2. At the time of retention in the system, the information will be labeled regarding its level of quality (accurate, complete, current, verifiable, and reliable).

3. The DSEMIIC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

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

5. The DSEMIIC will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system.

6. The DSEMIIC will conduct periodic data quality reviews of information it originates and make every reasonable effort, in a timely manner, to ensure that information will be changed or deleted from the system when it learns that 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 DSEMIIC. The recipient agency will receive written or electronic notification when information previously provided to them is deleted or changed by the center because the information is determined to be erroneous, is out of date, cannot be verified, or lacks adequate context such that an individual's rights may be affected.

7. The DSEMIIC will advise external originating agencies of their responsibility to review the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

H COLLATION AND ANALYSIS OF INFORMATION

1. Information acquired or received by the DSEMIIC 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 subject to collation and analysis is information as defined and identified in Section D.

2. Information sought or received by the DSEMIIC or from other sources will only be analyzed by qualified individuals to provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities generally. Additionally, to further crime (including terrorism) prevention, enforcement, force deployment, or prosecution objectives and priorities established by the DSEMIIC.

3. Information sought or received by the DSEMIIC or from other sources will not be analyzed or combined in a manner or for a purpose that violate Section E.

I MERGING OF INFORMATION FROM DIFFERENT SOURCES

1. 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 and hair color, race, ethnicity, tattoos, or scars; social security number; drivers license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may

include the name, federal or state tax ID number, office address, and telephone number.

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

J SHARING AND DISCLOSURE OF INFORMATION

1. Credentialed, role-based access criteria will be used by the DSEMIIC, as appropriate, to control:
   - The information to which a particular group or class of users can have access based on the group or class.
   - The information a class of users can add, change, delete, or print.
   - To whom, individually, the information can be disclosed and under what circumstances.

2. Access to information retained by the DSEMIIC will only be provided to persons within the DSEMIIC or in other governmental agencies or private sector entities who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with the law and procedures applicable to the DSEMIIC for whom the person is working.

   An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

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

4. The person who received, reviewed, or added information to the system may be authorized to view the information he or she provided regardless of the type of access associated with the information or the contributor's access authority.

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

6. Information retained by the DSEMIIC may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures.

The DSEMIIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself, unless otherwise required by law.

An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

7. Information gathered or collected and records retained by the DSEMIIC may be accessed or disseminated ***for specific purposes*** upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.

   The DSEMIIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself, unless otherwise required by law.

   An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed, and the specific purpose will be kept for a minimum of 5 years by the center.

8. The DSEMIIC will ensure that information gathered and retained by the DSEMIIC may be disclosed to a ***member of the public*** only if the information complies with the Michigan Freedom of Information Act and, where applicable, 5 U.S.C. 552a.

   The DSEMIIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself, unless otherwise required by law.

   An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

9. Information gathered or collected and records retained by the DSEMIIC will not be:
   - Sold, published, exchanged, or disclosed for commercial purposes.
   - Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
   - Disseminated to persons not authorized to access or use the information.

10. There are several categories of records that will ordinarily not be provided to the public:
    - Records required to be kept confidential by law M.C.L. § 15.243 (13) (d).
    - Information that meets the definition of “classified information” as that term is defined in 50 U.S.C. 401 et seq.
    - Investigatory records of law enforcement agencies. However, certain law enforcement records must be made available for inspection and copying. M.C.L. § 15.231 et seq.
    - 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 exempted from disclosure requirements under Michigan’s Freedom of Information Act – M.C.L.§15.231 et seq. 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. M.C.L.§ §15.243 (13) (d).
- A violation of an authorized nondisclosure agreement. M.C.L. § 15.243

K INFORMATION RETENTION AND DESTRUCTION

1. All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23, or for a longer or shorter period as specified by state law or local ordinance.

   Non-criminal intelligence information will be reviewed for record retention (validation or purge) by the DSEMIIC on an annual basis.

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

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

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

5. A record of information to be reviewed for retention will be maintained by the DSEMIIC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

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

L ACCOUNTABILITY AND ENFORCEMENT

L.1 Information System Transparency

1. The DSEMIIC will be open with the public in regard to information and intelligence collection practices. The center's privacy policy will be provided to the public for review upon request and the policy will be published on the center's Web site once established in accordance with the Freedom of Information Act and, where applicable, 5 U.S.C.552a. to the center's email address at fusion_center@detroitmi.gov or by written notification and posted on the center's Web site as soon as it is established.

The DSEMIIC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Officer (or the Executive Director) can be contacted at the following e-mail address: fusion_center@detroitmi.gov.

L.2 Accountability

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

2. The DSEMIIC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of (3) years of requests for access to information or specific purposes and of what information is disseminated to each person in response to the request.

3. The DSEMIIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least semi-annually and a record of audits will be maintained by the Executive Director of the center. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the agency's information

4. Personnel or other authorized users of the DSEMIIC shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Officer (Section C3).

5. The DSEMIIC will annually conduct an audit and inspection of the information contained in its information system(s). The audit will be conducted by the center's designated independent panel. This independent panel has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).

6. Guided by the appointed and trained Privacy Officer, the DSEMIIC Advisory Board will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

7. The DSEMIIC will notify an individual about whom encrypted personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens physical or financial harm to the person. The notice will be made promptly and without reasonable 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 to reasonably restore the integrity of the information system.

L.3 Enforcement

1. The DSEMIIC will require any individuals authorized to use the system to agree in writing to comply with the provisions of this policy and in the event of a conflict with the individual's participating agency policies, seek agency authorization prior to deviation from this policy.

2. If DSEMIIC personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the Executive Director of the DSEMIIC will:

   - Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user;

   - Suspend, demote, transfer, or terminate center personnel, as permitted by applicable personnel policies;

   - Apply administrative actions or sanctions as provided by (state agency or center) rules and regulations or as provided in agency/center personnel policies;

   - If the authorized user is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; OR

   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

3. The DSEMIIC 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.

M REDRESS

M.1 Disclosure

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in Section J.7, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the DSEMIIC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The DSEMIIC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

2. The existence, content, and source of the information will not be made available by the DSEMIIC to an individual about whom information has been gathered when:

- Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution [M.C.L. §15.243 (1) (b)];
- Disclosure would endanger the health or safety of an individual, organization, or community [M.C.L. §15.243 (13)];
- The information is in a criminal intelligence system subject to [28 CFR Part 23 and /or M.C.L. §15.243];
- The information source does not reside with the DSEMIIC [M.C.L. §15.231 et seq.]; or
- The DSEMIIC did not originate and does not have a right to disclose the information [M.C.L. §15.231 et seq.];
- Other authorized basis for denial [M.C.L. §15.243].

M.2 Complaints and Corrections

1. If an individual has complaints or objections to the accuracy or completeness of information about him/her originating with DSEMIIC that has been disclosed, the DSEMIIC's Privacy Officer will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

2. If an individual has complaints or objections to the accuracy or completeness of information about him or her that **originates with another agency**, the DSEMIIC will notify the source agency of the complaint or request for correction and its determination that disclosure by DSEMIIC or referral of the requestor to the source agency was neither required or appropriate under applicable law or refer the requestor to the originating agency, if appropriate or required. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

3. If an individual has complaints or objections to the accuracy or completeness of terrorism-related protected information that is exempt from disclosure, has been or may be shared through the ISE (1) is held by the DSEMIIC and (2) allegedly has resulted in demonstrable harm to the complainant, the DSEMIIC will inform the individual of the procedure for submitting (if needed) and resolving complaints and objections. Complaints will be directed to the DSEMIIC Privacy Officer at the following email address: fusion_center@detroitmi.gov. The DSEMIIC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence or non-existence of the information that is exempt from disclosure, as permitted by law. If the information did not originate with the DSEMIIC, the DSEMIIC will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. Any information held by the DSEMIIC or originating by the DSEMIIC will be reviewed within 30 days and confirmed or corrected/purged in or deleted from DSEMIIC data/records according to applicable records retention procedures if it is determined to be erroneous, include incorrectly merged information, or out of date. If there is no

resolution within 30 days, DSEMIIC will not share the information until such time as the compliant has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

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

M.3 Appeal

1. If an individual has objections to the accuracy or completeness of the information retained about himself or herself, the DSEMIIC will inform the individual of the procedure for requesting review of any objections. The individual will be given reasons if a request for correction is denied. The individual will also be informed of the procedure for appeal when the DSEMIIC has declined to correct challenged information to the satisfaction of the individual about whom the information relates.

   A record will be kept of all requests and of what information is disclosed to an individual.

N SECURITY SAFEGUARDS

1. The DSEMIIC's Executive Director is designated and trained to serve as the center's security officer.

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

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

4. The DSEMIIC 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.

5. The DSEMIIC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

6. Queries made to the DSEMIIC's data applications will be logged into the data system identifying the user initiating the query.

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

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

9. The DSEMIIC will notify an individual about whom personal 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.

O TRAINING

1. The DSEMIIC will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:

    - All assigned personnel to the DSEMIIC;
    - Personnel providing information technology services to the DSEMIIC;
    - Staff in other public agencies or private contractors providing services to the DSEMIIC; and
    - Users who are not employed by the DSEMIIC or a contractor.

2. The DSEMIIC will provide special training to personnel authorized to share protected information through the Information Sharing Environment regarding the agency's/center's requirements and policies for collection, use, and disclosure of protected information.

3. The DSEMIIC's privacy policy training program will cover:

    - Purposes of the privacy, civil rights, and civil liberties protection policy;
    - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the DSEMIIC;
    - How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
    - Originating and participating agency responsibilities and obligations under applicable law and policy;
    - The impact of improper activities associated with infractions within or through the DSEMIIC; and

- Mechanisms for reporting violations of center privacy protection policies and procedures; and

- The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

APPENDIX A TERMS AND DEFINITIONS

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.

Acquisition
The means by which an ISE participant obtains information through the exercise of 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
The Detroit & Southeast MI Information Center (DSEMIIC) and all agencies that access, contribute, and share information in the DSEMIIC's justice information system

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 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
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.

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 to topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Center
Center refers to the Detroit and Southeast MI Information Center and all participating state agencies of the Detroit and Southeast MI Information Center.

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 on government.

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

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

Confidentiality
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 activity. Criminal Intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

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

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, 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.

DSEMIIC
DSEMIIC refers to the Detroit and Southeast Michigan Information Center that's comprised of Federal, State, local, public, private, and tribal entities in the Southeast Michigan Region.

Fair Information Practices
The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECED) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:
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
8. Accountability Principle

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

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

Information
Information includes any data about people, organizations, events, incidents, or objects regardless of the medium in which it exists. Information received by law enforcement agencies

can be categorized into four general areas: general data, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information.

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

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

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

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

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

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 are getting access to the data. See also Audit Trail.

Metadata
In its simplest form, metadata is information (data) about information, more specifically information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to

facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

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

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.

Personal Data
Personal data refers to any information that relates to an identifiable individual (or data subject).

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).

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

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

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
As used in this policy, *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/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interest. 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
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 information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Michigan constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws and ordinances. Protection may be extended to organizations by DSEMIIC policy or state, local, or tribal law.

Public
Public includes any of the following:

- 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 DSEMIIC'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 DSEMIIC.

Public does not include:

- Employees of the DSEMIIC;
- People or entities, private or governmental, who assist the DSEMIIC in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the DSEMIIC is specified in law.

Purge
Purge refers to the deletion or destruction of information and data.

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

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

Retention
Refer to Storage.

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

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.

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:

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

Suspicious activity is defined in the ISE-SAR Functional Standard (version 1.5) as "observed activity and/or behavior that is believed to be indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Report (SAR)

Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information

Consistent with Section 1016(a)(4) of 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 Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as recently amended by the 9/11 Commission Act enacted on 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

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.

Tips and Leads Information or Data

Generally uncorroborated reports or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview reports (FIRs) 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 is 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 has some suspicion or is based on a level of suspicion that is less than "reasonable suspicion," but 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.

APPENDIX B LAWS, REGULATIONS, AND REFERENCES

(FEDERAL)

United States Constitution

United States Constitution, First Amendment, U.S. Const. Am. 1
United States Constitution, Fourth Amendment, U.S. Const. Am. 4
United States Constitution Fourteenth Amendment, U.S. Const. Am. 14

Statutes

Brady Handgun Violence Prevention Act, 18 U.S.C.§§ 921, 922, 924, and 925A, United States Code, Title 18, Part 1, 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-1-05, "Guidance on Interagency Sharing of Personal Data—Protecting Personal Privacy," December 20, 2000

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

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

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 Act, 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

Homeland Security Act of 2002, 6 U.S.C.§481-482(F)(1)

Indian Civil Right Act of 1968, 25 U.S.C. §1301, United States Code, Title 25, Chapter 15, Subchapter I, §1301
Intelligence Identities Protection Act of 1982, 50 U.S.C. §421 United States Code, title 50, Chapter __, Subchapter __§421

Internal Security Act of 1950, (ISA) also know as the Subversive Control Act or the McCarran Act, 50 U.S.C. §783, United States Code, Title 50 Chapter __, Subchapter___, §783

Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA), *as amended by the 9/11 Commission Act*; also referenced as the National Security Intelligence Reform Act. 50 U.S.C. §401 Untied States Code Title 50, Chapter __, Subchapter ____, §401

Law Enforcement Intelligence Systems, 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

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

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

USA PATRIOT Act, 18 U.S.C. 1 *et seq*. [Public Law NO 107-56 (October 26, 2001), 115 Stat. 272] United States Code Title 18, Chapter ___, §1 *et seq*

US Criminal Laws, including 18 USC 641, 783, 793, 794, 952, 1924, 2721

Regulations

Classified Information, 32 CFR 2003

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

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

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 I, Volume 2, Part 46

Presidential /Executive Orders

Presidential Executive Order 13526 – Classified National Security Information

(STATE - MICHIGAN)

Michigan Constitution 1963 - Article 24 as amended December 24, 1988

Michigan Constitution 1963 – Article 27 as amended December 19, 2008.

Statutes

Child identification and protection Act, M.C.L. §722.771 et seq. Michigan Compiled Laws 722.711-722.775

Insurance Code – Privacy of Financial Information, M.C.L. §500.501 et seq. Michigan Compiled Laws §500.501-500.547

Michigan Emergency Management Act, M.C.L. §30.401 et seq. Michigan Compiled Laws §30.401

Michigan Freedom of Information Act, M.C.L. §15.231 et seq. Michigan Compiled Laws §15.231

National Crime Prevention and Privacy Compact M.C.L. §3.1051 et seq. Michigan Compiled Laws §3.1051 -3.1053

Preservation of Personal Privacy Act, M.C.L. §445.1711 et seq. Michigan Compiled Laws §445.1711-445.1715

Social Security Number Privacy Act, M.C.L. §445.81 et seq. Michigan Compiled Laws §445.81 -445.87

Executive Orders

Gubernatorial Executive Order 2007-47 (Granholm) Establishing The Michigan Intelligence Operations Center For Homeland Security Department Of State Police

Gubernatorial Executive Order 2009-52 (Granholm) Protecting Michigan's Homeland Security

APPENDIX C RECEIPT OF DSEMIIC PRIVACY POLICY

Receipt of DSEMIIC Privacy Policy
By DSEMIIC and Non-DSEMIIC Personnel

My signature below indicates that I have been provided a copy, have read and that I understand the Detroit and Southeast Michigan Information Center Privacy Policy. I understand that the Privacy Policy applies to me and that its violation may serve as a basis for a disciplinary action, up to and including dismissal.

Signature: _____

Printed Name: _____

Date Signed: _____