UD-040 (10/02)
MEMORANDUM

STATE OF MICHIGAN
DEPARTMENT OF STATE POLICE

DATE: August 3, 2015

TO: Michigan Intelligence Operations Center (MIOC) Staff

FROM: D/F/Lt. Brian Budde, Commander, MIOC

SUBJECT: Privacy Policy

MIOC PRIVACY POLICY

A. PURPOSE

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

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 2012-5 Establishing the Michigan Intelligence Operations Center for Homeland Security.

In support of this Executive Order 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 Commander /Director of ***MIOC*** within the MSP. The ***MIOC*** is guided by an agency-designated privacy committee that is available to interact 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 led by a trained privacy officer who is appointed by the commander/director of the ***MIOC.*** 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 Information

Sharing Environment (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, working through the Commander 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

  Email: 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 or activity 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).

- 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
- Does not interfere with or compromise pending criminal investigations.
- Protect individual's right of privacy, civil rights, and civil liberties.
- 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.

- 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 (Which is information about the information- origins, nature, validity and such See App A) 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

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 employed. An electronic, data based audit trail sufficient to allow the identification of each individual who accessed information retained by the ***MIOC*** will be kept by the ***MIOC***. The MIOC Security officer will maintain records of MIOC visitors who access information as part of their authorized visits.

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. MIOC products include an advisory statement informing external agencies of this proviso.

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 involved, or when there is a legitimate need. An audit trail SHALL be kept by the MIOC Privacy Officer 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 or agencies not authorized to access or use the information.

There are several categories of records that will not ordinarily be provided to the public 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 sec 13 (d));
- the information source does not reside within the ***MIOC*** (when information is not disclosed because it did not originate within 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 or regulation.

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 within 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*** Privacy Officer of all complaints and the resulting action taken in response to the complaint.

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.

MIOC personnel will not investigate a request for correction or any complaint made by any person other than the subject of the record or alleged record in question.

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 protected 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 with security that is the same as, or similar to, the system that secures data rising to the level of reasonable suspicion. In order to prevent disclosure to the public, 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 (validate 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, or both, 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 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 upon request.

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.

APPLICABILITY

This policy applies to **ALL *MIOC*** personnel and partners.

This policy is incorporated into the ***MIOC***'s standard operating procedures and complies with the *State of Michigan's Information Sharing Environment Base Policy and Procedures*, and the ***MIOC*** Intrastate Coordination Plan. It is the ***MIOC*** Commander's responsibility to ensure compliance with this policy and procedure(s). This plan was created on 10/13/2011 and is updated on an "as needed basis" and is audited annually on the creation anniversary date. All changes are reflected in the REVISION section of this policy.

POLICY ENFORCEMENT

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

REVISION RESPONSIBILITY

The responsibility for revision of this policy lies with the ***MIOC*** Training and Development Unit Policy Officer and approved by the ***MIOC*** Commander.

Appendix A to MIOC Privacy Policy

TERMS and DEFINITIONS

Actionable Information:

Information that results in an intelligence analytical product or dissemination based on *immediate action* (where there is imminent danger); or *action where there is need for follow-up but is non-imminent* or is for *informational purposes only.*

Analysis:

That activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment. *(Source: Baseline Capabilities for State and Major Urban Area Fusion Centers--Sep. 2008)*

Baseline Capability:

A capability provides the means to accomplish a mission or function resulting from the performance of one or more critical tasks, under specified conditions, to target levels of performance. A capability may be delivered with any combination of properly planned, organized, equipped, trained, and exercised personnel that achieves the desired outcome. (Source: *National Preparedness Guidelines,* pg. 40) Within the context of this document, *Baseline capabilities for Fusion Centers* is a capability necessary for the fusion center to perform its core functions of gathering, processing, analyzing, and disseminating terrorism, homeland security, and law enforcement information. *(Source: Baseline Capabilities for State and Major Urban Area Fusion Centers-Sep. 2008)*

Baseline Capabilities Assessment:

A formal nationwide assessment of *Fusion Centers*- baseline capabilities in order to better understand the strength and maturity of the National Network of Fusion Centers. The 2010 inaugural assessment was conducted by the Program Manager for the Information Sharing Environment, in coordination with Fusion Center Directors, the Department of Homeland Security, the Federal Bureau of Investigation, and other federal interagency partners.

Classified Information/Intelligence:

A uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism, to ensure that certain information is maintained in confidence in order to protect citizens, U.S. democratic institutions, U.S. homeland security, and U.S. interactions with foreign nations and entities. (Source: *Baseline Capabilities for State and Major Urban Area fusion centers*)

Critical Operational Capability (COC) Gap Mitigation Maturity Model:

The scale against *which fusion center's* progress toward the achievement of the COC is being assessed as part of the Baseline Capabilities Assessment. The three levels include:

1. *Defined and Above*: *The fusion center* has documented plans, policies, and processes in place to achieve the COC
2. *Below Defined/Refinement*: The fusion center has processes in place, but need additional resources to help document their processes; and
3. *Below Defined/Fundamentals*: The fusion center needs resources to help develop and document plans, policies, and processes.

Confidentiality Agreement:
A written agreement between the fusion center and the recipient of information produced by that fusion center, for appropriate confidentiality of the information shared.

Critical Operational Capability (COC):
During the 2010 National Fusion Center Conference, *Fusion Center* partners distilled the *Baseline Capabilities for State and Major Urban Area Fusion Center*s into eight key priority areas for *Fusion Center*s: four COCs and four enabling capabilities. Maturing the COCs is essential to building an integrated National Network *of Fusion Centers*. The four COCs include:

1. *Receive*: Ability to receive classified and unclassified information from federal partners
2. *Analyze*: Ability to assess the local implications of threat information through the use of a formal risk assessment process
3. *Disseminate*: Ability to further disseminate threat information to other state, local, tribal, and territorial and private sector entities within the MIOC's jurisdiction; and
4. *Gather*: Ability to gather locally-generated information, aggregate it, analyze it, and share it with federal partners, as appropriate.

Federally-Generated Information:
Time-sensitive threat information that may take the form of alerts, warnings, notifications, or other products that should be accessed, reviewed, and appropriately disseminated in a timely manner.

For Official Use Only (FOUO):
A term used to identify unclassified information of a sensitive nature, not otherwise categorized by statue or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest. FOUO is not to be considered classified information. FOUO material should be stored in a closed container when not in use and disposed of by shredding or burning when no longer useful. Disseminated FOUO material must include proper handling instructions.

Fusion Process:
The overarching process of managing the flow of information and intelligence across levels and sectors of government and private industry. It goes beyond establishing an information/intelligence center or creating a computer network. The Fusion Process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. The Fusion Process turns information and intelligence into actionable knowledge. (Source: Fusion Center *Guidelines*, August 2006)

Fusion Process Capabilities:
The Fusion Process Capabilities identify those capabilities and standards necessary to perform the steps of the Intelligence Process within a fusion center including the gathering, analysis, and dissemination of information and intelligence. Though the steps and actions of the Fusion Process do not comprehensively mirror the steps of the Intelligence Process, the Intelligence Process provides the foundation to carry out the Fusion Process and assist in the identification of the capabilities needed to successfully complete the Fusion Process. (Source: *Baseline Capabilities for State and Major Urban Area* fusion centers- *Sep. 2008*)

Homeland Security – State and Local Intelligence Communities of Interest (HS–SLIC):
A secure information network platform that supports the sharing of non-classified information between fusion centers and the Federal Government.

Information:
Pieces of raw, unanalyzed data that identify persons, evidence, or events or illustrate processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event. (Source: Baseline Capabilities for State and Major Urban Area fusion center's *Sep. 2008*)

Information Sharing Environment (ISE):
A trusted partnership among all levels of government, the private sector, and foreign partners to detect, prevent, preempt, and mitigate the effects of terrorism against territory, people, and interests of the United

States of America. This partnership enables the trusted, secure, and appropriate exchange of terrorism information, in the first instance, across the five federal communities; to and from state, local, and tribal governments, foreign allies, and the private sector; and at all levels of security classifications. (Source: Baseline Capabilities for State and Major Urban Area fusion centers, *Sep. 2008*)

Intelligence (Criminal):
The product of the analysis of raw information related to crimes or crime patterns with respect to an identifiable person or group of persons in an effort to anticipate, prevent, or monitor possible criminal activity (or investigate or prosecute). (Source: Baseline Capabilities for State and Major Urban Area fusion centers- *Sep. 2008*)

Intelligence Analyst:
A professional position in which the incumbent is responsible for taking the varied facts, documentation of circumstances, evidence, interviews, and any other material related to a crime and organizing them into a logical and related framework for the purposes of developing a criminal case, explaining a criminal phenomenon, describing crime and crime trends, and/or preparing materials for court and prosecution, or arriving at an assessment of a crime problem or crime group. *(Source: Baseline Capabilities for State and Major Urban Area Fusion Centers-Sep. 2008)*

Intelligence Community:
Agencies of the U.S. Government identified by statute and Executive Order, including intelligence elements of the U.S. Department of Defense, that have the responsibility to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national and homeland security of the United States. These activities include, in part, the collection of information and the production and dissemination of intelligence. (50 U.S.C. § 401a; Section 3 of the National Security Act of 1947, as amended).

Intelligence Products:
Reports or documents that contain assessments, forecasts, associations, links, and other outputs from the analytic process that may be disseminated for use by law enforcement agencies for the prevention of crimes, target hardening, apprehension of offenders, and prosecution. (Source: Baseline Capabilities for State and Major Urban Area Fusion Centers- *Sep. 2008*)

ISE Shared Spaces Concept or Shared Spaces:
The ISE Shared Spaces concept is a key element of the *ISE Enterprise Architecture Framework* and helps resolve the information-processing and usage problems identified by the 9/11 Commission. ISE Shared Spaces are networked data and information repositories used by ISE participants to make their standardized terrorism-related information, applications, and services accessible to other ISE participants. ISE Shared Spaces also provide an infrastructure solution for those ISE participants with national security system (NSS) network assets, historically sequestered with only other NSS systems, to interface with ISE participants having only civil network assets. Additionally, ISE Shared Spaces provide the means for foreign partners to interface and share terrorism information with their U.S. counterparts. For more information about the ISE Shared Spaces concept, reference the *ISE Enterprise Architecture Framework* and the *ISE Profile Architecture and Implementation Strategy* at www.ise.gov. (Source: Baseline Capabilities for State and Major Urban Area fusion centers *Sep. 2008*)

Law Enforcement On-Line (LEO):
A secure information sharing network supplied to law enforcement officers, sponsored by the Federal Bureau of Investigation (FBI).

Law Enforcement Sensitive (LES):
Unclassified information from a law enforcement agency that contains personal identifying information, such as victim, suspect, business, or information that might be used in a criminal prosecution that requires protection against unauthorized disclosure to protect the sources, methods, investigative activity,

evidence, and the integrity of the investigation reports. The exception to this is when an active arrest warrant is on file and personal identifiers have been released outside of law enforcement.

Metadata:
Metadata describes other data. It provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data.

Law Enforcement Intelligence:
The end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgments and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution or project crime trends or support informed decision making by management. (Source: Baseline Capabilities for State and Major Urban Area Fusion Centers- *Sep. 2008*)

National Intelligence or Intelligence Related to National Security:
Defined by Section 3 of the National Security Act of 1947, as amended, as "A) information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" (known as foreign intelligence); and B) "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (known as "counterintelligence"), regardless of the source from which derived and including information gathered within or outside the United States, that (A) pertains to more than one United States Government agency; and (B) involves (i) threats to the United States, its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on the United States national or homeland security." (50 U.S.C. § 401a) The goal of the National Intelligence effort is to provide the President and the National Security [Staff] with the necessary information on which to base decisions concerning the conduct and development of foreign, defense, and economic policy and the protection of United States national interests from foreign security threats. (Executive Order 12333)

National Law Enforcement Telecommunications System (NLETS):
A secure information sharing platform used by law enforcement.

Planning:
The preparation for future situations, estimating organizational demands and resources needed to attend to those situations, and initiating strategies to respond to those situations. (Source: Baseline Capabilities for State and Major Urban Area Fusion Centers- *Sep. 2008*)

Policy:
The principles and values that guide the performance of a duty. A policy is not a statement of what must be done in a particular situation. Rather, it is a statement of guiding principles that should be followed in activities which are directed toward the attainment of goals. (Source: *Baseline Capabilities for State and Major Urban Area* Fusion Centers- *Sep. 2008*)

Privacy (Information):
The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of personally identifiable information will be adhered to by criminal justice agencies, with use of such information to be strictly limited to circumstances in which the legal process permits use of the personally identifiable information. (Source: *Baseline Capabilities for State and Major Urban Area* Fusion Centers- *Sep. 2008*)

Privacy (Personal):
The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of behaviors of an individual – including his/her communications, associations, and transactions – will be adhered to by criminal justice agencies, with the use of such information to be strictly limited to circumstances in which legal process authorizes surveillance and investigation. (Source: *Baseline Capabilities for State and Major Urban Area* Fusion Centers- *Sep. 2008*)

Requirements (Information or Intelligence):
The types of intelligence operational law enforcement elements need from the intelligence function within an agency or other intelligence-producing organizations in order for law enforcement officers to maximize protection and preventive efforts as well as identify and arrest persons who are criminally liable. *(Source: Baseline Capabilities for State and Major Urban Area Fusion Centers-Sep. 2008)*

Regional Information Sharing System (RISS):
A secure information sharing platform used by federal, state and local law enforcement agencies.

Regional Information Sharing System, Automated Trusted Information Exchange (RISS ATIX):
A secure information sharing platform used by federal, state, and local law enforcement to communicate with appropriately identified stakeholders within government agencies and critical infrastructure.

Reporting:
Depending upon the type of intelligence, the process of placing analyzed information into the proper form to ensure the most effective consumption. (Source: *Baseline Capabilities for State and Major Urban Area Fusion Centers- Sep. 2008*)

Risk Assessment:
The product of three principal variables: Threat – the likelihood of an attack occurring and Vulnerability and Consequence – the relative exposure and expected impact of an attack. Risk assessment is the process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact on an asset. It is a function of threat, vulnerability, and consequence. A risk assessment may include scenarios in which two or more risks interact to create greater or lesser impact. A risk assessment provides the basis for the rank ordering of risks and for establishing priorities for countermeasures. Risk is classically represented as the product of a probability of a particular outcome and the results of that outcome. A statewide or regional risk assessment assesses the threats, vulnerabilities, and consequences faced by the fusion centers geographic area of responsibility. The risk assessment is used to identify priority information requirements for the fusion center and to support state and urban area homeland security preparedness planning efforts to allocate funding, capabilities and other resources. In traditional criminal intelligence, a risk assessment means an analysis of a target, illegal commodity, or victim to identify the probability of being attacked or criminally compromised and to analyze vulnerabilities. (Source: *Baseline Capabilities for State and Major Urban Area Fusion Centers- Sep. 2008*)

Short-Term Critical Operational Capability (COC) Gap Mitigation Objectives:
Short-term COC gap mitigation objectives are aligned to each of the COCs and represent the focus of mitigation efforts through December 2010. These include:

Receive: Develop and implement a written plan for the receipt of federally-generated time sensitive threat information

Analyze: Develop and implement a written plan to assess the local implications of time-sensitive and emerging threat information

Disseminate: Develop and implement a written plan identifying the dissemination of time sensitive and emerging threat information to all homeland security partners, including law enforcement and other disciplines; and

Gather: Develop and implement a written plan to gather locally-generated information, including suspicious activity reporting, based on time-sensitive and emerging threats.

Suspicious Activity:
Reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention. (Source: *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*, June 2008; and ISE-SAR Functional Standard version 1.0)

Suspicious Activity Report:
Official documentation of reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention. (Source: *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*, June 2008; and ISE-SAR Functional Standard version 1.0)

Target:
Any person, organization, group, crime or criminal series, or commodity being subject to investigation and intelligence analysis. *(Source: Baseline Capabilities for State and Major Urban Area Fusion Centers—Sep.2008)*

Target Profile:
The identification of crimes, crime trends, and crime patterns that have discernable characteristics which make collection and analysis of intelligence information an efficient and effective method for identifying, apprehending, and prosecuting those who are criminally responsible. (Source: *Baseline Capabilities for State and Major Urban Area Fusion Centers- Sep. 2008)*

"To Target" or "Targeting":
"To target" or "targeting" as used in this document refers to planning, intelligence collection, reconnaissance, physical/electronic surveillance, and similar activities by threat groups to carry out an attack against any Sector or Key Resource.

Threat Assessment:
An assessment of a criminal or terrorist presence within a jurisdiction integrated with an assessment of potential targets of that presence and a statement of probability that the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal's or terrorist's opportunity, capability, and willingness to fulfill the threat. (Source: *Baseline Capabilities for State and Major Urban Area Fusion Centers- Sep. 2008*)

Vulnerability Assessment:
An assessment of possible criminal or terrorist group targets within a jurisdiction integrated with an assessment of the target's weaknesses, likelihood of being attacked, and ability to withstand an attack. *(Source: Baseline Capabilities for State and Major Urban Area Fusion Centers--Sep. 2008)*

Warning:
To notify in advance of possible harm or victimization as a result of information and intelligence gained concerning the probability of a crime or terrorist attack. (Source: *Baseline Capabilities for State and Major Urban Area Fusion Centers- Sep. 2008*)

Appendix B to MIOC Privacy Policy

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'/MIOCs' 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/MIOCs 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

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

IRTPA, 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 § 1385, http://www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap67-sec1385 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

Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5

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

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