MAINE STATE POLICE
MAINE INFORMATION & ANALYSIS CENTER
PRIVACY POLICY

(EFFECTIVE DATE: 03.20.2019)

TABLE OF CONTENTS

PART		PAGE
I.	Mission Statement & Guiding Principles of the Maine Information and Analysis Center	3
II.	Governance of the MIAC	3
III.	Policy Applicability	5
IV.	Terms and Definitions	5
V.	Information Management & Security	6
VI.	Information Quality	11
VII.	Collation & Analysis of Information	13
VIII.	Access to & Disclosure of Information	15
IX.	Information Retention & Destruction	20
X.	Accountability, Enforcement, and Security	21
XI.	Training	24
XII.	Appendix A—Federal and SLTT Laws, Regulations, and Guidance Relevant to Seeking, Retaining, and Disseminating Justice Information	27
XIII.	Appendix B—Terms and Definitions	30
XIV.	Appendix C—Fair Information Practice Principles	40

Part I. Mission Statement & Guiding Principles of the Maine Information and Analysis Center

Mission Statement

A. The mission of the Maine Information and Analysis Center ("MIAC") is – for criminal justice, national security, and public safety purposes only – to seek, acquire, and receive information, analyze such information, and, when lawful and appropriate, retain and disseminate such information to individuals and agencies permitted access to the information.

Guiding Principles

B. In carrying out its work, the MIAC shall:

1. Protect privacy, civil rights, civil liberties, and other protected interests of all individuals;
2. Minimize the threat and risk of injury to specific individuals and groups;
3. Minimize the threat and risk of damage to real and personal property;
4. Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;
5. Minimize the threat and risk of physical and financial injury to law enforcement and others responsible for public protection, safety, and health;
6. Increase public safety and improve national security; and
7. Comply with laws protecting privacy, civil rights, and civil liberties[1].

Part II. Governance of the MIAC

MIAC Director

A. The Lieutenant attached to the MIAC is the MIAC Director.

[1] The Constitutions of the United States of America and of the State of Maine guarantee, among other rights, Freedom of Speech, Freedom of the Press, and Freedom of Peaceable Assembly. Therefore, law enforcement responses to incidents involving the exercise of such rights must focus on whether criminal activity and/or suspicious activity has occurred or is occurring at such incidents. Determinations of whether any such activity has occurred or is occurring must be based on specific, articulable facts relating to criminal activity. As warranted by the circumstances, MIAC may provide support to law enforcement agencies engaged in normal criminal investigations and may work with other agencies to discharge of law enforcement's public safety mission, including MIAC's role with assisting in or responding to information- and intelligence-related inquiries that officers may have in response to a First Amendment-protected event or activity.

B. The MIAC Director shall have primary responsibility for the operation of the MIAC.
C. The MIAC Director is responsible for –

1. All MIAC information technology system ("MIAC ITS") operations;
2. Coordinating and managing MIAC personnel;
3. Acquiring, retaining, evaluating, assessing the quality of, analyzing, destroying, sharing, and disclosing information maintained by the MIAC;
4. Enforcing the provisions of this policy;
5. Community outreach.

D. The MIAC Director may be contacted at the following email address: intel.msp@maine.gov, attention "MIAC Director."

MIAC Privacy Officer

E. The Maine State Police Staff Attorney is the MIAC Privacy Officer.
F. The MIAC Privacy Officer shall be trained as described in Part XI of this policy.
G. The MIAC Privacy Officer is to be responsible for –

1. Assisting with implementing the requirements of this policy;
2. Ensuring that privacy, civil rights, and civil liberties are protected as provided in this policy and by the center's information acquisition, retention, and dissemination processes;
3. Receiving reports regarding alleged errors and violations of the provisions of this policy;
4. Receiving and responding to inquiries about privacy, civil rights, and civil liberties protections of the information systems maintained or accessed by the center;
5. Reviewing and recommending updates to this policy every calendar year in response to changes in law and implementation experience, including the results of audits and inspections;
6. Receiving and processing complaints about privacy, civil rights, and civil liberties protections in accordance with this policy, and at the direction of the MIAC Director;
7. Consulting with and assisting the MIAC Compliance Officer in conducting audits of the center every calendar year;
8. Ensuring that enforcement procedures and sanctions outlined in this policy are adequate and enforced.

H. The MIAC Privacy Officer may be contacted at the following email address: intel.msp@maine.gov, attention "MIAC Privacy Officer."

MIAC Compliance Officer

I. The Sergeant attached to the MIAC is the MIAC Compliance Officer.
J. The MIAC Compliance Officer is responsible for –

1. Conducting required audits of the center in consultation with the MIAC Privacy Officer every calendar year;
2. Ensuring, in consultation with the MIAC Privacy Officer, that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies;
3. Investigating suspected or known misuse of information or intelligence in the custody of the MIAC;
4. Investigating suspected or known violations of the provisions of this policy.

K. The MIAC Compliance Officer may be contacted at the following email address: intel.msp@maine.gov, attention "MIAC Compliance Officer."

MIAC Security Officer

L. The Sergeant attached to the MIAC is the MIAC Security Officer.

M. The MIAC Security Officer is responsible for –

1. Maintaining a record of all privacy, civil rights, and civil liberties training received by any personnel subject to this policy, as described in Parts XI;
2. Collecting and maintaining the written acknowledgements that MIAC personnel are required to complete pursuant to this policy in order to be authorized to use any MIAC ITS;
3. Determining whether data/information breaches and security breaches have occurred when he or she becomes aware that any such breach might have occurred. If any such breach is determined to have occurred, the Security Officer shall determine whether notifications must be made to affected individuals and, if such notifications are needed, the MIAC Security Officer shall provide, or cause to have provided, those notifications;
4. Maintaining a record of all audits conducted pursuant to this policy after being provided with such records by the MIAC Compliance Officer.

N. The MIAC Security Officer may be contacted at the following email address: intel.msp@maine.gov, attention "MIAC Security Officer."

MIAC Advisory Board

O. To ensure that the individual privacy, civil rights, and civil liberties of all individuals remain protected, the administration of the MIAC shall be advised by a MIAC Advisory Board, which shall be responsible for reviewing new and revised written P/CRCL policies of the MIAC.

1. The MIAC Director shall convene the board at least once every twelve (12) months.

Part III. Policy Applicability

A. This policy applies to all authorized MIAC personnel, participating agency personnel, information-technology services support personnel, and contractors. This policy applies to information in the custody and control of the MIAC that the center acquires, collects, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment ("ISE") participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

B. MIAC personnel and participating agency personnel, as well as information-technology services support personnel, and contractors that have direct access to the MIAC facility or any MIAC ITS shall protect individuals' rights as guaranteed by the United States of America and Maine Constitutions and other applicable laws protecting privacy, civil rights, and civil liberties.[2]

C. MIAC has adopted internal operating policies that are in compliance with the laws listed in Footnote 2.

D. The MIAC shall provide access to an electronic copy of this policy to MIAC personnel and participating agency personnel, as well as to information-technology services support personnel and contractors that have direct access to MIAC information or any MIAC ITS. MIAC shall require both a written acknowledgement of receipt of this policy and a written agreement to comply with the provisions contained in this policy. Prior to being able to access to systems, MIAC personnel and participating agency personnel, as well as information-technology services support personnel and contractors that have direct access to MIAC information or any MIAC ITS shall provide such documentation to the MIAC Security Officer.
    a. Users are subject to the terms of use stated on the MIAC Law Enforcement Secure Portal.

E. This policy shall be accessible worldwide via the Internet.

Part IV. Terms and Definitions

[2] Statutory civil rights protections established pursuant to the U.S. Constitution may, in addition, directly govern State action. These include, but are not limited to, 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. The U.S. Constitution, Federal laws, Executive Orders, regulations, and policies, including, but not limited to, 28 CFR Part 23 and the Health Insurance Portability and Accountability Act (HIPAA), may potentially affect the sharing of information, including sharing terrorism-related information in the information sharing environment. In addition to the Maine Constitution, MIAC personnel shall also adhere to the Maine Criminal History Record Information Act (16 M.R.S. c. 7), the Maine Intelligence and Investigative Record Information Act (16 M.R.S. c.9), and Maine law regarding the interception of wire and oral communications (*see* 15 M.R.S. c. 102). *See* Appendix A for the laws, regulations, and guidance relevant to seeking, retaining, and disseminating justice information.

For examples of primary terms and definitions used in this policy, refer to Appendix B, Terms and Definitions.

Part V. Information Management & Security

A. In administering any MIAC ITS, the MIAC shall only seek, acquire, retain, or share information that:

1. Is based on a criminal predicate or possible threat to public safety; or
2. Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal conduct or activity that presents a threat to any individual, the community, or any nation, and the information is relevant to the criminal conduct or activity; or
3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
4. Is useful in a crime analysis or in the administration of criminal justice and public safety; and
5. The source of the information is reliable and verifiable, or limitations on the quality of the information are identified; and
6. The information was collected in a fair and lawful manner.

B. The MIAC may retain information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or SAR information, subject to applicable provisions in this policy.

C. The MIAC shall not intentionally seek, acquire, retain, or share 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 event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

1. When participating on a federal law enforcement task force or when documenting a Suspicious Activity Report ("SAR") or an Information Sharing Environment–SAR ("ISE-SAR") in the NSI, race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity shall not be considered as factors creating suspicion; however, those attributes may be documented in specific suspect descriptions for identification purposes.

D. The MIAC shall ensure that the source of all information acquired and retained by the center in accordance with this policy is appropriately documented.

Labeling/Description of Information

E. When analyzing information received through or entered into a MIAC ITS or a criminal intelligence system, MIAC personnel shall assess the information to determine its nature, usability, and quality.

F. At the time a decision is made by the MIAC to add information to a MIAC ITS, the information must be labeled to the maximum extent feasible and reasonable, and pursuant to applicable limitations on access and sensitivity of disclosure, in order to:

1. Protect confidential sources and police undercover and/or investigative techniques, methods, and procedures;
2. Not interfere with or compromise pending criminal investigations;
3. Protect individuals' rights of privacy and their civil rights and civil liberties;
4. Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

G. The labels assigned and/or descriptions given to existing information under this "Labeling/Description of Information" section must be reevaluated whenever:

1. New information is added that is known to have a material impact on access limitations or the sensitivity of disclosure of the information;
2. There is a known change in the use of the information materially affecting access or disclosure limitations (for example, the information becomes part of court proceedings for which there are different public access laws).

H. The MIAC may incorporate the SAR process into existing processes and systems used to manage other crime-related information and criminal intelligence.

Methods of Acquiring Information

I. Information gathering and investigative techniques used by the MIAC shall comply with all applicable laws.

J. The MIAC shall not intentionally directly or indirectly seek, acquire, or retain information from a nongovernmental information provider, or a commercial database, that may or may not receive a fee or benefit for providing the information, if the center knows or has reason to believe that:

1. The individual or information provider is legally prohibited from acquiring the specific information sought or disclosing it to personnel within the center;[3]
2. The individual or information provider used methods for acquiring the information that MIAC personnel could not legally use;[4] or

[3] An exception to this is if the individual did not act as an agent of, or at the direction of, any bona fide law enforcement officer participating with the center.

3. It is known that the specific information sought from the individual or information provider could not legally be acquired by any MIAC personnel.

K. External agencies that access a MIAC ITS or otherwise share information with the center are governed by the laws and rules governing those individual agencies, including, but not limited to, applicable federal and state laws.

L. To the extent it will do so at all, the MIAC shall contract only with commercial database entities that ***certify in writing*** prior to providing contracted-for services or products:

1. That their methods for gathering personally identifiable information comply with applicable laws and regulations; and
2. That their methods are not based on misleading information-gathering practices.

Basic Descriptive Information

M. Basic descriptive information shall be used when entering information into a MIAC ITS and electronically associated with data (or content) for which there are known to be special laws, rules, or policies regarding access, use, and disclosure, including, but not limited to, terrorism-related information shared through the ISE.

1. To the extent reasonably known or ascertainable, the types of information should include:

a. The name of the originating agency, with reasonable specificity as to the division or unit of the agency from which the information originates;
b. The name of the originating agency's justice information system from which the information is disseminated;
c. The date the information was collected by the center and, where feasible, the date its accuracy was last verified;
d. The title or position, and contact information of, the person to whom questions regarding the information should be directed.

Received tips and leads, including, but not limited to, Suspicious Activity Reporting ("SAR") Information

N. The center may receive tips and leads, including, but not limited to, SAR information.

[4] An exception to this is if the individual did not act as an agent of, or at the direction of any bona fide law enforcement officer participating in the center. In such a case, the MIAC Director shall seek the advice of the Maine State Police Staff Attorney regarding any legal restrictions before any information is used or shared in any way.

O. MIAC shall use the MIAC Activity Report to document and categorize SAR information the center acquires.

1. Such information shall be maintained in the Activity Report as follows:

a. An analyst who receives SAR information (either by e-mail, phone, or in person) shall create an Activity Report entry and indicate the date and time the information was received.

(1) The analyst shall indicate in the appropriate fields from which agency and/or person the information originated, and shall include that person's contact information.

b. The analyst shall categorize the "nature of the request" as a "SAR."
c. The analyst then shall categorize the "reason for the request" appropriately, given the nature of the information, as well as the facts and circumstances contemplated in the information.
d. The analyst then shall sub-categorize the request appropriately, given the nature of the information and the underlying facts and circumstances contemplated in the information.
e. In the "free-text" narrative field, the analyst then shall state his or her work activity associated with the information.
f. The analyst also shall attach any relevant supporting documentation he or she acquires when the SAR information is received, processed, and entered into the Activity Report, such as – as examples only – results of database checks, requests for information, and police reports.
g. The analyst shall create additional supplements to the original entry with any informational updates.

2. MIAC personnel shall adhere to the following procedures when acquiring, assessing, storing, disclosing, retaining, and securing tips and leads information, including, but not limited to, SARs:

a. Prior to disclosing such information, MIAC personnel shall ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence.
b. MIAC personnel shall allow access to or disclose such 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 PII).
c. MIAC personnel shall regularly provide access to or disclose such 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.

d. MIAC personnel shall maintain SAR information in its Activity Report in the MIAC ITS, using in the same or substantially similar manner as information that rises to the level of reasonable suspicion is secured and that includes an audit and inspection process, supporting documentation, and labeling of the data, in accordance with Section V(E) – (H) (above) to delineate it from other information.

e. MIAC personnel shall adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips and leads, including, but not limited to, SAR information.

3. In its collection and maintenance of SAR information, to the extent reasonably feasible and consistent with MIAC's legal authorities and mission requirements, the MIAC shall:

a. Identify and review protected information that may be accessed from or disclosed by the center prior to sharing the SAR information through the ISE; and
b. Include notice mechanisms to enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

P. Information acquisition and investigative techniques used by the MIAC and participating agency personnel exchanging information with the center must be in compliance with and adhere to applicable laws, including, but not limited to:

1. 28 CFR Part. 23, as applicable;
2. The FIPPs (see Appendix C, but note that under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act, state, local, tribal, or territorial law, or center policy);
3. Federal and state constitutional provisions; and
4. Maine statutes and regulations.

Q. When processing SAR information, the center shall provide for human review and vetting to ensure that the information is both legally acquired and, where applicable, determined to have a potential nexus to terrorist activity.

1. MIAC personnel shall be trained to recognize those behaviors and incidents that are indicative of criminal activity associated with terrorism.

R. When processing SAR information, the center shall include safeguards to ensure, to the greatest degree possible, that only information regarding individuals and organizations involved in activities that have been determined to be consistent with terrorist activity is documented and shared through the ISE.

1. Such safeguards are intended to ensure that information that could violate civil rights and civil liberties will not be intentionally or inadvertently acquired, documented, processed, and shared. See Part V.(A) – (D) of this policy.

Part VI. Information Quality

A. To the extent reasonably feasible, the MIAC shall ensure that information sought, acquired, and retained by the center is:

1. Derived from dependable and trustworthy sources of information;[5]
2. Accurate;
3. Current;
4. Complete (including the relevant context in which it was sought or received and other related information);[6]
5. Merged with other information about the same individual or organization only when the applicable standard has been met.

B. MIAC shall implement a process for additional fact development during the vetting process where a SAR includes PII and is based on behaviors that are not inherently criminal. MIAC shall articulate additional facts or circumstances to support the determination that the behavior observed is reasonably indicative of preoperational planning associated with terrorism.

C. The MIAC shall investigate, in a timely manner, alleged errors and deficiencies (or refer them to the originating agency) and will correct, delete, or refrain from using protected information found to be erroneous or deficient.

D. All criminal intelligence information entries or submissions made to MIAC criminal intelligence system shall be reviewed by the MIAC to ensure they meet the submission requirements of 28 CFR Part 23.

E. The MIAC shall establish a deadline by which the information entered into or submitted to a criminal intelligence system must be reviewed and validated for a new retention period by the user or agency submitting the information.

1. If the established deadline is not met, or the user contributing the information cannot be reached in a timely manner, the information shall be deleted.

[5] This may include commercial databases, in addition to participating agencies.

[6] Open source information, public information, or a source with an unknown reliability may be sought, acquired, and retained by the MIAC, but shall be noted as such and a disclaimer shall be added to the information that indicates (1) that the information may not be accurate, and (2) that the recipient should independently assess and verify the content of the information before any official action is taken based on the result of the information.

F. To the extent reasonably feasible and consistent with agency authorities and mission requirements, MIAC will provide notice of whether information in an ISE-SAR, terrorism-related analytic product, or criminal intelligence information record/product:

1. Is subject to specific information privacy or other similar restrictions on access, use or disclosure,[7] and if so, the nature of such restrictions; and
2. Has limitations on the reliability or accuracy of the information.

G. If MIAC or participating agency personnel exchanging information through a MIAC ITS or criminal intelligence system have a concern, or are notified of a concern by another agency member, regarding source reliability, or if information is in error such that it may affect a person's rights or civil liberties, the MIAC Compliance Officer shall be promptly notified of the concern.

1. The MIAC Compliance Officer shall review the allegation in accordance with this policy.

    a. The MIAC Compliance Officer shall provide the MIAC Director with a written report on each source reliability investigation on which the MIAC Compliance Officer works.

H. The MIAC Director shall maintain a record of sources determined not to be reliable to ensure they are not used by the MIAC until the reliability issues have been resolved.

I. The MIAC shall conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information is corrected, deleted from a MIAC ITS, or not used when the center:

1. Identifies information that is erroneous, misleading, obsolete, or – in light of the totality of attendant circumstances – unreliable;
2. Discovers that it did not have authority to gather the information or to provide the information to another agency; or
3. Used prohibited means to gather the information.[8]

J. MIAC personnel shall notify the MIAC Director and the MIAC Compliance Officer that information maintained in a MIAC ITS must be corrected or deleted by the MIAC when such personnel learns and confirms that:

1. The information is erroneous, misleading, obsolete, unreliable, improperly merged, or lacks adequate context such that the rights of the individual may be affected;

[7] See, e.g., Maine Criminal History Record Information Act, 16 M.R.S. c. 7; and Maine Intelligence and Investigative Record Information Act, 16 M.R.S. c. 9.

[8] Except when the center's information source did not act as the agent of the center in gathering the information.

2. The source of the information did not have authority to gather the information or to provide the information to the center;[9]
3. The source of the information used prohibited means to gather the information, except when the source did not act as an agent at to a bona fide law enforcement officer.

K. To the extent reasonably feasible, if the MIAC Director learns that criminal intelligence information or potential terrorism-related information received by the MIAC is alleged, suspected, or found to be materially inaccurate, incomplete, or out of date, the Director shall contact the appropriate contact person at the participating agency that provided that information and make the participating agency aware of the problem with the information. Participating agency personnel are solely responsible for reviewing the quality and accuracy of the information provided to the MIAC.

L. If erroneous information provided from a commercial database is included in a MIAC ITS, the MIAC Director shall notify the privacy office or appropriate contact of the commercial database business.

M. The MIAC shall notify recipient agencies when information previously disclosed to them through a MIAC ITS is known to have been deleted or changed pursuant to this policy.

1. Such notifications must be made in writing, and the fact the notification was made (and the date on which it was made) shall be documented by the MIAC.

2. The MIAC shall establish physical and electronic safeguards to ensure that only authorized users are allowed to add, change, or delete information in a MIAC ITS.

Part VII. Collation & Analysis of Information

Collation and Analysis

A. Information subject to collation and analysis is information as defined and identified in Part V of this policy. Information that is acquired by the MIAC or from other sources shall only be analyzed for purposes consistent with this policy:

1. By MIAC personnel who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly;

[9] Except when the source did not act as an agent to a bona fide law enforcement officer, and only if the rules of criminal procedure and prevailing State and Federal case laws allows it, and only after consultation with Maine State Police Staff Attorney and/or the Maine Office of the Attorney General.

2. 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 activities generally; and
3. To further crime prevention, enforcement, force deployment, or prosecution objectives and priorities; or
4. For activity that may pose a threat to the public safety, including, but not limited to, the safety of law enforcement officers and criminal justice agency personnel.

B. Information acquired by the MIAC or accessed from other sources is analyzed according to priorities and needs, and shall be analyzed only to:

1. Further crime prevention (including, but not limited to, terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center;
2. 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, but not limited to, terrorist) activities.

Merging of Information from Different Sources

C. Information shall be merged with other information maintained by the MIAC only by qualified individuals who meet the criteria set forth in Part VII(A) of this policy.
D. Information about an individual or organization from two or more sources shall not be purposefully merged in a MIAC ITS or criminal intelligence system unless there is sufficient identifying information to clearly establish that the information is about the same individual or organization.
E. The set of identifying information sufficient to allow merging in a MIAC ITS or criminal intelligence system shall consist of available attributes that can contribute to higher accuracy of match, but should have at least three matches.

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

Pre-disclosure Review of Certain MIAC-created Intelligence Products

F. As requested by MIAC personnel, the MIAC Privacy Officer shall review intelligence products created by the MIAC to ensure that they provide appropriate privacy, civil rights, and civil liberties protections, before such products are disclosed by the center.

Part VIII. Access to & Disclosure of Information

A. The MIAC shall use credentialed, role-based access criteria, as appropriate, to control:

1. The information in a MIAC ITS to which a particular group or class of users can have access based on the group or class;
2. The information a class of users of a MIAC ITS can add, change, delete, or print; and
3. To whom, individually, the MIAC ITS information may be disclosed, and under what circumstances.

B. The MIAC shall adhere to the current version of the *ISE-SAR Functional Standard* for the SAR process when ISE-SAR information is involved.

The MIAC shall maintain records of agencies sharing information with the MIAC and employ system mechanisms to identify the originating agency when the information is shared with the MIAC.

C. Direct access to any information retained by the MIAC only shall be provided to individuals authorized to have such access.

1. Each instance of access to or disclosure of information in a MIAC ITS shall be manually or electronically documented.

    a. The documentation must identify each individual who accessed or acquired information maintained by the center and explain the nature of the information accessed.

D. A MIAC ITS may be accessed only when the system is capable of providing an audit trail to the administrators in the center.

1. Each such instance of access to a MIAC ITS shall be manually or electronically documented.

E. Agencies external to the MIAC may not disclose information accessed through or disclosed from a MIAC criminal intelligence system without the prior approval of the center or the originator of the information.

F. Except as otherwise provided in this policy or required by applicable public records access laws, access to or disclosure of information maintained by the MIAC only shall be disclosed to persons within the center or in other governmental agencies who are authorized to have such access, and only for:

1. Legitimate law enforcement, public protection, prosecution, public health, or justice purposes; and
2. The performance of official duties in accordance with law and procedures applicable to the agency for which the person is working.

To the extent reasonably feasible, the MIAC shall electronically or manually document such disclosure to identify who or what agency requested and/or received the information. Such documentation must be maintained by the MIAC for a minimum of seven (7) years.

Disclosing Information to the Public in the Aid of Investigation

G. Information acquired and/or maintained by the MIAC may be disclosed to the public or media if the information is a public record, or if the release of the information, if protected, might aid a criminal investigation or ensure for the safety of the public.

    1. Each such disclosure must be manually or electronically documented, and such documentation must be retained by the MIAC for a minimum of seven (7) years.

Inability Confirm the Existence or Nonexistence of Intelligence and Investigative Record Information

H. The MIAC cannot confirm the existence or nonexistence of intelligence or investigative information to any person or agency that would not be eligible to receive the information itself. *See* 16 M.R.S. §§ 803(7), 804, 807.

Disclosing Information to an Individual about Whom Information Has Been Acquired

I. Upon satisfactory verification of an individual's identity (e.g., through fingerprinting the individual, through the presentation by the individual of a valid, government-issued identification), and subject to the conditions specified in this policy and applicable law (including, *inter alia*, 16 M.R.S. §§ 807 and 808), an individual may learn of the information about him or her that is maintained by the MIAC.

    1. Subject to applicable law (*see, inter alia*, 16 M.R.S. §§ 807 and 808), the individual may review and, to the extent permitted by law, obtain a copy of, the information maintained about him or her, for the purpose of challenging the accuracy or completeness of the information.
    2. The center's response to such requests shall be made to the requesting individual by the MIAC Privacy Officer within (thirty (30) days) after the receipt of the request.
    3. Subject to applicable law (*see inter alia* 16 M.R.S. §§ 807 and 808), if the information about the individual making the request did not originate with the MIAC, either:

        a. The individual shall be referred to the originating agency, if legally permissible; or

b. The center shall inform the individual making the request that the center cannot confirm the existence or nonexistence of the information.

(1) In such circumstances, the center shall notify the originating agency of the request and of the center's determination that confirmation of the existence of the information by the MIAC, and the referral of the individual making the review request to the originating agency, was not legally permissible.

4. A record must be kept of each request made by individuals to review information about them that is maintained by the MIAC.

a. When applicable, the record must describe the information that was reviewed by the individual that made the request.

J. There are categories of records to which the public will not be provided access, and these include, but are not limited to, the following:

1. Records and information that by law are designated as confidential;

a. Such records and information include, but are not limited to, investigatory records of law enforcement agencies that are exempted from disclosure requirements under the Maine Criminal History Record Information Act (16 M.R.S. c. 7) and the Maine Intelligence and Investigative Record Information Act (16 M.R.S. c. 9).

(1) However, such investigatory records of law enforcement agencies must be made available for inspection and copying to the extent permitted under those Acts;

2. Records that by definition of law are not "public records" (*see* 1 M.R.S. § 402(3));
3. Information that meets the definition of "classified information," as that term is defined in the National Security Act, Public Law 235, Section 606 and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010;
4. A record or part of a record that, if publicly disclosed, would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under the Maine Intelligence and Investigative Record Information Act (16 M.R.S. c. 9);
5. Governmental agency records that are protected by law and, as a matter of law, cannot be disclosed publicly.

K. Except as permitted under applicable law, the existence, content, and source of the intelligence and investigative record information shall not be disclosed to an individual if there is a reasonable possibility that release or inspection of the information would result in one or more harms listed at 16 M.R.S. § 804, sub-§§ 1 – 12.

Requests for the Correction of Information that has been Disclosed Publicly

L. If an individual requests correction of information originating with the MIAC that has been disclosed (including, but not limited to, disclosed to the individual him- or herself) by the MIAC, the individual shall submit the objection to the MIAC Director at the following email address: intel.msp@maine.gov.

M. The MIAC Director shall forward the objection to the MIAC Privacy Officer, who, within fifteen (15) business days after receiving the objection, shall notify the person filing the objection that the objection has been received.

N. Within thirty (30) business days after receiving the objection, the MIAC Privacy Officer shall conduct an investigation to determine whether correction of the information at issue is warranted, in whole or part, and then report his or her findings to the MIAC Director.

O. Within fifteen (15) business days after receiving the MIAC Privacy Officer's findings, the MIAC Director shall make the final decision about whether the information will be corrected in whole or part.

1. The individual making the request for the correction of the information shall be notified in writing of the MIAC Director's decision.

    a. If the decision is made by the MIAC Director that the information is not to be corrected in whole or part, the MIAC Director shall inform the individual in writing of each reason the information will not be corrected in whole or part.
    b. At such time, the individual also will be informed that the MIAC Director's decision may be appealed in writing to the Colonel of the Maine State Police within thirty (30) days after the decision is rendered.

2. If an individual timely appeals the MIAC Director's decision to the Colonel of the Maine State Police, the Colonel shall reconsider and render a decision regarding the MIAC Director's decision within forty-five (45) business days after the written appeal is received by the Colonel.

    a. In reconsidering the MIAC Director's decision, the Colonel may consult with the Maine Office of the Attorney General.
    b. The Colonel's decision to uphold in whole or part, or reverse, the MIAC Director's decision constitutes final agency action.

P. The final disposition of each such request for correction must be documented and kept on file by the MIAC for at least seven (7) years.

Complaints Regarding Terrorism-related Protected Information

Q. If an individual has a complaint regarding the accuracy or completeness of terrorism-related protected information that:

1. Is exempt from disclosure; or
2. Has been or may be shared through the Information Sharing Environment; and

    a. Is maintained by the MIAC; and
    b. Allegedly has resulted in demonstrable harm to the individual making the complaint,

then the MIAC shall inform that individual that he or she may submit the complaint to the MIAC Director at the following e-mail address: intel.msp@maine.gov, to the attention of the "MIAC Director."

3. Upon the receipt of such a complaint, the MIAC Director shall forward the complaint to the MIAC Privacy Officer.
4. Within fifteen (15) business days after the MIAC's receipt of the complaint, the MIAC Privacy Officer shall notify the person filing the complaint that the complaint has been received.
5. Within thirty (30) business days after the MIAC's receipt of the complaint, the individual shall be notified of the MIAC's response to and determination regarding the complaint.

    a. The determination shall be made by the MIAC Director in consultation with the MIAC Privacy Officer.

6. At such time that the individual is notified of the MIAC Director's decision, the individual also shall be informed that the decision may be appealed in writing to the Colonel of the Maine State Police within thirty (30) days after the decision is rendered.
7. If an individual timely appeals the MIAC Director's decision to the Colonel of the Maine State Police, the Colonel shall reconsider and render a decision regarding the MIAC Director's decision within forty-five (45) business days after the written appeal is received by the Colonel.

    a. In reconsidering the MIAC Director's decision, the Colonel may consult with the Maine Office of the Attorney General.
    b. The Colonel's decision to uphold in whole or part, or reverse, the MIAC Director's decision constitutes final agency action.

R. The final disposition of each such request for correction must be documented and kept on file by the MIAC for at least seven (7) years.

Prohibited uses of information

S. Information acquired and retained by the MIAC **SHALL NOT BE**:

1. Sold, published, exchanged, or disclosed for commercial purposes;
2. or
3. Disseminated to persons not authorized to access or use the information.

Part IX. Information Retention & Disposition

Review of Information Regarding Retention

A. All criminal intelligence information shall be reviewed for record retention (validation or purge) by the MIAC at least every five (5) years from the date it was received by the MIAC.

B. All other information maintained by the MIAC shall be retained in accordance with the MIAC retention schedules. See http://www.maine.gov/sos/arc/records/state/policy.html.

C. When information maintained in a MIAC ITS has no further value or meets the criteria for removal under the center's retention and destruction policy, it shall be disposed of in accordance with applicable retention schedules.

1. Information shall not be returned to the submitting source.

Destruction of Information

D. The MIAC shall purge criminal intelligence information from a criminal intelligence system operated by MIAC, unless it is reviewed and validated, at least every five (5) years from the date it was entered in or submitted to a criminal intelligence system that is subject to 28 CFR Part 23.

E. Notification to or approval by originating and participating agencies of proposed destruction or return of records or information is not required.

1. Originating and participating agencies that have maintained their own copies of records or information submitted to the MIAC are solely responsible for auditing and purging such records in accordance with applicable law and policy.

F. No record of information purged from a criminal intelligence system operated by MIAC shall be maintained by the MIAC, to satisfy the integrity and completeness of the purged information from appropriate systems, with the exceptions of information stated in this policy.

Destruction of Classified National Security Information

G. Classified information ("Secret") maintained by the MIAC shall be reviewed on an annual basis.
H. This review shall:

1. Determine if there is a continuous use/need for each classified document kept by the MIAC;
2. Ensure that ALL classified materials being retained have the appropriate classified cover sheets attached;
3. Ensure that ALL classified materials being retained are properly marked;
4. Ensure that ALL Secret materials are recorded on Classified Material Control Inventory Form CD-481;
5. Ensure that ALL Secret materials selected for destruction are recorded on the form CD-481 and are destroyed by approved methods.

Part X. Accountability, Enforcement, and Security

Information System Transparency

A. The MIAC shall be open with the public regarding information and intelligence gathering, collection, retention, and dissemination practices, to the extent permitted by state law. The center's P/CRCL policy will be provided to the public for review upon request, and posted on the MIAC's website http://www.maine.gov/miac/.

Accountability for Activities

B. The MIAC shall establish and implement procedures, practices, system protocols, and use of software, information technology tools, and physical security measures that protect each MIAC ITS from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions.

1. Access to a MIAC ITS from outside the facility shall be allowed only over secure networks.

C. The MIAC shall store MIAC ITS information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions, as designated by the MIAC Director.

D. The MIAC shall adopt and follow procedures and practices by which it can ensure and evaluate the compliance of individuals who are subject to this policy with the terms of this policy and with applicable law.

1. This shall include manual or electronic logging access of these systems that ensures that the identities of users of the systems, and an auditable trail of data accessed by MIAC personnel is created.

2. An audit trail must be kept for a minimum of seven (7) years of requests for access to information for specific purposes and of what information is disclosed to each person in response to the request.
3. These systems shall be reviewed every calendar year by the MIAC Compliance Officer, and a record of the reviews must be maintained by the MIAC Director.

    a. The MIAC shall adopt and follow procedures by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law.
    b. Audits:

        (1) Must be conducted every calendar year by an independent third party or alternatively, by the MIAC Compliance Officer in consultation with the MIAC Privacy Officer;
        (2) May include any type of medium (printed and electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related MIAC activity;
        (3) Must be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s);
        (4) Must be performed in a manner so as to not establish a pattern of the audits.

    c. A record of the audits shall be maintained by the MIAC Compliance Officer, as well as by the MIAC Security Officer.
    d. Appropriate elements of the audit process and key audit outcomes must be compiled into a report by the Compliance Officer in consultation with the MIAC Privacy Officer, and must be provided to the MIAC Director, the Maine State Police Command Staff, and the MIAC Advisory Board.

E. Direct access to a MIAC ITS shall be granted only to the MIAC 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.
F. To prevent their unauthorized disclosure, risk and vulnerability assessments shall not be stored with publicly available data.
G. Individuals who are subject to this policy and who become aware of any of the circumstances identified below shall report the matter to the MIAC Compliance Officer. This includes:

    1. Any errors and suspected or confirmed violations of center policies relating to protected information; and
    2. Any suspected or confirmed data breaches (in any medium or form, including paper, oral, and electronic) as soon as possible and without

unreasonable delay, consistent with applicable laws, regulations, policies, and procedures.

a. *See* definitions of "data breach," "originating agency," "protected information," and "personally identifiable information" in Appendix B.

H. The MIAC Compliance Officer shall annually review, or cause to have reviewed, the information maintained in each MIAC ITS.

1. The results of each such review must be shared with the MIAC Advisory Board.
2. The review must be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of information maintained in all MIAC ITS.

I. In response to updates in applicable law and public expectations, the MIAC shall review the provisions of this policy protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes.

1. The MIAC Director shall maintain records of such reviews and, upon request, make them available for audits and to the MIAC Advisory Board.

J. Data/Information Breach Procedures

1. Data Breaches involving PII:

a. As soon as practicable following assessment of a suspected or confirmed data breach of PII in a MIAC ITS, the MIAC Security Officer shall notify the originating agency from which the center received PII of the nature and scope of a suspected or confirmed breach of such information.

(1) *See* definitions of "Personally Identifiable Information" and "Data Breach" in Appendix B.

2. Security Breach involving Personal Information:

a. With regard to security breaches that involve personal information stored in a MIAC ITS, the MIAC adheres to the requirements and procedures set forth in 10 M.R.S. § 1346 *et seq*.
b. In accordance with 10 M.R.S. § 1346, *et seq*., the MIAC Security Officer shall determine whether a security breach involving a MIAC ITS requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures and, if such notification is needed, the MIAC Security Officer shall provide, or cause to have provided, that notification.

(1) *See* definitions of "Personal Information" and "Security Breach" in Appendix B.

c. Required notifications shall 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 MIAC information system affected by this release.

Enforcement

K. If an individual who is subject to this policy is found not to be complying with the provisions of this policy regarding the acquisition, use, retention, destruction, sharing, classification, or disclosure of information, the MIAC Director shall investigate and may:

1. Suspend or discontinue access to information by the individual;
2. Apply administrative actions or sanctions as provided by applicable laws and policies of the State of Maine;
3. If the individual is from an agency outside of the Maine State Police, request that the agency employing the individual initiate proceedings to discipline the user or enforce this policy's provisions; or
4. Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of this policy.

Right to Restrict Access to MIAC Information and Facilities

L. The MIAC reserves the right to restrict the qualifications and number of individuals having access to center-maintained information and center facilities, as well as to suspend or withhold service and deny access to any participating agency personnel.

Part XI. Training

Personnel requiring training and frequency

A. The MIAC shall require each individual to whom this policy applies to review the policy and acknowledge in writing that such review has occurred, and that the individual understands and agrees to abide by the applicable terms of the policy.
B. MIAC personnel shall review this policy as necessary to carry out their duties lawfully and appropriately; whenever the policy is amended or revised; and when directed to do so by the MIAC Director.

1. The MIAC shall provide appropriate, role-based training to MIAC personnel authorized to disclose protected information through the ISE regarding the MIAC's requirements and policies for acquisition, collection, use, and disclosure of protected information.
2. To the extent reasonably feasible, the MIAC Privacy Officer, MIAC Compliance Officer, and the MIAC Security Officer each shall receive the additional training, in addition to the training provided under section 3 of this Part, below, appropriate to the respective positions.

C. The initial training program content for MIAC personnel training shall include:

1. The purposes of this policy;
2. The substance and intent of the provisions of the policy relating to acquisition, use, analysis, retention, destruction, sharing, and disclosure of information retained by the MIAC in a MIAC ITS or criminal intelligence system, as appropriate;
3. The impact of improper activities associated with MIAC ITS information accessible within or through the MIAC;
4. The nature and possible penalties for violations of this policy, including possible administrative, civil, and criminal liability;
5. Originating and participating agency responsibilities and obligations under applicable law and this policy;
6. How to implement this policy in the day-to-day work of the user;
7. Potential impact of violations of this policy and mechanisms for reporting violations of the policy;
8. How to identify, report, and respond to a suspected or confirmed breach of PII;
9. Updates to this policy, if any, in response to changes in law and implementation experience; and
10. Subject to course availability and funding, the MIAC Privacy Officer also shall take courses offered by the Department of Homeland Security or other federal partners addressing:

    a. Privacy, civil rights, and civil liberties training of trainers;
    b. Derivative classification marking; and
    c. ISE Core Awareness Training.

The MIAC Director will determine the training courses that are feasible and appropriate for other individuals to whom this policy applies.

Record of Training

D. Individuals who are subject to the training provisions of this policy are responsible for providing a record of the training to the MIAC Security Officer.
E. The MIAC Security Officer shall maintain a record of all privacy, civil rights, and civil liberties training received by MIAC personnel.

APPENDIX A

FEDERAL AND SLTT LAWS, REGULATIONS, AND GUIDANCE RELEVANT TO SEEKING, RETAINING, AND DISSEMINATING JUSTICE INFORMATION

The U.S. Constitution is the primary authority that applies to federal as well as state, local, tribal, and territorial (SLTT) agencies. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution, but states can broaden constitutional rights guaranteed by their own constitutions.

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.[10]

In addition, statutory civil rights protections in the U.S. Constitution may 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.

The development of a privacy, civil rights, and civil liberties policy is primarily designed for center personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the center must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in a center P/CRCL policy, staff and user accountability is greatly diminished; mistakes are made; privacy, civil rights, and civil liberties violations occur; and the public's (and other agencies') confidence in the ability of the center 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.

It is important to note that federal laws may use different terminology to describe information that identifies an individual (e.g., personal data, personal information, information in identifiable form). Different laws may have different statutory definitions for the terminology used. Personnel who are charged with developing or updating their center's P/CRCL policy should refer to the applicable statutory definition, in order to ensure that the scope of the terminology used is properly understand and implemented.

1. Federal Laws, Regulations, and Guidance

Following are synopses of federal laws, regulations, and guidance that a center should review and, when appropriate, cite within the policy when developing a P/CRCL policy

[10] The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the Information Sharing Environment is explored in a key issues guidance paper titled *Civil Rights and Civil Liberties Protection*, which is available on the ODNI's Office of Partner Engagement-Information Sharing Environment (PE-ISE) website at www.ise.gov.

for a justice information system. The list is arranged in alphabetical order by popular name.

a. **Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611—**This statute provides a general overview of the Interstate Identification Index System (IIIS), an information sharing system that contains state and federal criminal history records that are also used for non-criminal justice purposes, such as governmental licensing and employment background checks. Congress recommends the creation of interstate and federal-state agreements to ensure that uniform policies are in place for records exchanges for non-criminal justice purposes and to prevent unauthorized use and disclosure of personal information due to variances in authorized users' policies. This statute is applicable to multijurisdictional information sharing systems that allow non-criminal justice-related exchanges.

b. **Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23—**This is a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to operate criminal intelligence systems effectively while safeguarding privacy, civil rights, and civil liberties during the collection, storage, and dissemination of criminal intelligence information. The regulation governs the intelligence information systems' process, which includes information submission or collection, secure storage, inquiry and search capability, controlled dissemination, and review and purge processes.

c. **Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20—**This applies to all state and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations and funded by the Omnibus Crime Control and Safe Streets Act of 1968, codified at 42 U.S.C. § 3789D. The regulation requires those criminal justice information systems to submit a criminal history information plan and provides guidance on specific areas that should have a set of operational procedures. These areas include completeness and accuracy of criminal history records and limitations on dissemination, including general policies on use and dissemination, juvenile records, audits, security, and access and review.

d. **Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721—**Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records—Collected License Plate Reader (LPR) information contains no PII that may be used to connect a license plate detection to an individual. It is only with permissible purpose that law enforcement may make this connect (using other systems), and this access is governed by the Driver's Privacy Protection Act of 1994. www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap123-sec2721/content-detail.html

e. **Federal Civil Rights Laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983—**This is a federal statute that allows an individual to sue public officials in federal court for violations of the individual's civil rights. Civil rights include such things as the Fourth Amendment's prohibitions against unreasonable search and seizure, violations of privacy rights, and violations of the right to freedom of religion, free speech, and free association. It serves as a deterrent to unlawful collection, use, or sharing of information rather than providing specific authority or a prohibition to the collection, use, or sharing of information.

f. **Federal Driver's Privacy Protection Act (DPPA), 18 USC § 2721-2725—** Restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of persons whose records have been obtained by that department in connection with a motor vehicle record unless certain criteria are met.

g. **U.S. Constitution, First, Fourth, Fifth, Sixth, and Fourteenth Amendments—**The Bill of Rights establishes minimum standards for the protection of the civil rights and civil liberties of individuals in the United States. The First Amendment protects religious freedom, speech, the press, the right to peaceably assemble, and the right to petition the government for a redress of grievances. The Fourth Amendment protects the people from unreasonable searches and seizures and requires that warrants be issued only upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the individual or things to be seized. The Sixth Amendment establishes the right of an accused individual to a speedy and public trial by an impartial jury, to be informed of the nature and cause of the charges, to confront witnesses, to have compulsory process to obtain witnesses, and to have the assistance of legal counsel. The Fourteenth Amendment addresses citizenship rights and equal protection of the laws. Although the equal protection clause applies explicitly only to state governments, equal protection requirements apply to the federal government through the Fifth Amendment Due Process Clause.

2. State Laws, Regulations, and Guidelines

a. **The Constitution of the State of Maine;**
b. **The Maine Freedom of Access Act, 1 M.R.S. c. 13;**
c. **Notice of Risk to Personal Data, 10 M.R.S. c. 210-B;**
d. **The Maine Criminal History Record Information Act, 16 M.R.S. c. 7;**
e. **The Maine Intelligence and Investigative Record Information Act, 16 M.R.S. c. 9;**
f. **State Police, 25 M.R.S. Pt. 4;**
g. **Homeland Security Advisory Council, 37-B M.R.S. § 708;**
h. **Executive Order 24 FY 06/07 (Effective 08 December 2006).**

Appendix B

Terms and Definitions

A. Unless the context expressly indicates otherwise, the key terms used in this policy shall be interpreted in accordance with Appendix B, Terms and Definitions.

1. Access. "Access" means the ability to get to (usually having permission to use) particular information on a computer. Web access means having a connection to the Internet through an access provider or an online service provider. With regard to the Information Sharing Environment ("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.
2. Acquisition. For purposes of the Information Sharing Environment ("ISE"), "acquisition" means the method by which an ISE participant obtains information through the exercise of its authority, but 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.
3. Authorized. "Authorized" means formally approved by the MIAC or in accordance with law.
4. Center. "Center" means the Maine Information & Analysis Center.
5. Civil liberties. "Civil liberties" means fundamental individual rights, such as freedom of speech, press, or religion; freedom from unreasonable search and seizure; 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, i.e., the first ten Amendments to the Constitution of the United States and the Constitution of the State of Maine. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.
6. Civil rights. The term "civil rights" means those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities shall take action to ensure that individuals are not discriminated against on the basis of any federally- or state- protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.

7. Contractor. "Contractor" means any person working for the MIAC on a contractual basis who, by virtue of his or her work, shall have direct, authorized access to any MIAC ITS.
8. Criminal intelligence information. "Criminal intelligence information" means information or data that has been evaluated to determine that it is 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, and meets criminal intelligence system submission criteria, as set forth in *CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES* (28 Code of Federal Regulations Part 23 ("28 C.F.R. Part 23")).

    a. Only those criminal intelligence records that meet the reasonable suspicion criteria and the other 28 CFR Part 23 operating principles and are shared between agencies by an intelligence project are subject to the regulation. Fact-based or uncorroborated information (case investigative files, case management systems, incident/offense reports, field interview cards or contact files, criminal history records, arrest blotters, records management system [RMS] data, tips and leads, suspicious activity reports [SARs], etc.) and other types of information or intelligence gathered/collected and shared by state, local, tribal, or territorial law enforcement and intelligence agencies are not subject to 28 CFR Part 23.

9. Criminal Intelligence System: For purposes of this policy, the term "criminal intelligence system" refers to a system that stores criminal intelligence information, as that term is defined in 28 CFR § 23.3(b)(1). The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to operate criminal intelligence information systems effectively while safeguarding privacy and civil liberties. The regulation applies to state, local, tribal, or territorial agencies if they are operating interjurisdictional or multijurisdictional criminal intelligence systems that are supported with Omnibus Crime Control and Safe Streets Act funding. See 28 CFR Part § 23.3(a). It may also apply as a matter of state law, grant conditions, or agency policy.
10. Data Breach. "Data breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII, or (2) an authorized user accesses or potentially accesses PII for a purpose other than the authorized purpose.
11. Disclosure. "Disclosure" means the release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner — electronically, orally, or in writing — to an individual, agency, or an organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information that may be available only to certain people for certain purposes but that is not available to everyone.

12. Fair Information Practice Principles. "Fair Information Practice Principles" ("FIPPs") means a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be of limited applicability in intelligence operations, as fusion centers do not generally engage with individuals. That said, fusion centers and all other integrated justice systems should endeavor to apply the FIPPs where practicable. The eight FIPPs are:

    a. Purpose Specification;
    b. Data Quality/Integrity (see definition at Appendix C);
    c. Collection Limitation/Data Minimization;
    d. Use Limitation;
    e. Security Safeguards (see definition at Appendix C);
    f. Accountability/Audit;
    g. Openness/Transparency;
    h. Individual Participation;

    See Appendix C for further background on the FIPPs.

13. Governmental agency. "Governmental agency" means, as applicable in the context of this policy, a county, municipal, state, territorial, tribal, or federal government agency.
14. Information. "Information" means any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists, that is collected, acquired, maintained, accessed, or disclosed, or disseminated by the MIAC directly and exclusively.

    a. Information received by law enforcement agencies can be categorized into three general areas:

        (1) General data, including investigative information;
        (2) Tips and leads data (including suspicious activity reports); and
        (3) Criminal intelligence information.

b. Information disseminated by the MIAC through means other than a MIAC ITS, e.g., through RISS network systems or databases, is regulated by the laws and policies applicable to such systems.

15. Information Sharing Environment. "Information Sharing Environment" ("ISE") means a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of governmental agencies and the private sector to facilitate terrorism-related information sharing, disclosure, and collaboration.
16. Information Sharing Environment Suspicious Activity Report. Information Sharing Environment Suspicious Activity Report ("ISE-SAR") means 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).
17. Information-technology services support personnel. "Information-technology services support personnel" means any State of Maine employee or contractor assigned to provide direct information technology services support for any MIAC IT system.
18. Law enforcement information. For purposes of the Information Sharing Environment ("ISE"), "law enforcement information" means any information acquired by or of interest to a law enforcement agency or official that is both (a) related to crime or the security of the United States, 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 in 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.
19. Maintenance of information. "Maintenance of information" refers to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic storage systems (for example, filing cabinets).

    a. To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

20. MIAC personnel. "MIAC personnel" means any person employed or contracted by or assigned as part of his or her official duties to the MIAC, and is either working in the MIAC physically or has direct, authorized access to a MIAC IT system.
21. MIAC Director. "MIAC Director" means the Director of the MIAC (*see* Part II, § 1), or his or her authorized designee.
22. MIAC information technology system. "MIAC information technology system" ("MIAC ITS") means any information technology system exclusively administered and maintained by or on behalf of the MIAC (e.g., MIAC Activity Report, Netsential). A MIAC ITS is not a criminal intelligence system.
23. Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI): The NSI establishes standardized processes and policies that provide the capability for Federal, state, local, tribal and territorial, campus, and railroad law enforcement and homeland security agencies to share timely, relevant ISE-SARs through a distributed information sharing system that protects privacy, civil rights, and civil liberties.

24. Nationwide Suspicious Activity Report ("SAR") Initiative ("NSI-SAR") SAR Data Repository. NSA-SAR SAR Data Repository means a single data repository, built to respect and support originator control and local stewardship of data, which incorporates federal, state, and local retention policies.

    a. Within the NSI SDR, hosted data enclaves extend this approach to information management and safeguarding practices by ensuring a separation of data across participating agencies.

25. Need to know. "Need to know" means, as a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for an individual to have in order to conduct his or her official duties as part of an organization, and the individual has a right to know the information in order to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.
26. Originating Agency. "Originating Agency" means the agency or organizational entity that documents information, including source agencies that document Suspicious Activity Report ("SAR") (and, when authorized, Information Sharing Environment–SAR ("ISE-SAR")) information that is collected by a fusion center.
27. Participating agency. "Participating Agency" means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system.

28. Personally identifiable information. "Personally identifiable information" ("PII") means any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[11]

29. Personal Information. "Personal information" means an individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

    a. Social security number;
    b. Driver's license number or state identification card number;
    c. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;
    d. Account passwords or personal identification numbers or other access codes; or
    e. Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

    "Personal information" does not include information from third-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. *See* Title 10 MRS § 1347(6).

30. Preoperational Planning. As defined in Information Sharing Environment–Suspicious Activity Report ("ISE-SAR") Functional Standard 1.5.5, "preoperational planning" means activities associated with a known or particular planned criminal operation or with terrorist operations generally.

31. Protected information. "Protected information" means personally identifiable information about individuals that is subject to information privacy and/or other legal protections under the Constitution and the laws of the United States.

    a. Protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes (such as civil rights laws) and regulations,

[11] For further information about the breadth of PII and how to perform an assessment of the specific risk that an individual can be identified using the information, *see* Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

including, but not limited to, 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, tribal, and territorial laws, ordinances, and codes.

b. Protection may be extended to individuals and organizations by federal or Maine law or executive order, or the terms of this policy.

32. Public record. "Public record" means "any written, printed or graphic matter or any mechanical or electronic data compilation from which information can be obtained, directly or after translation into a form susceptible of visual or aural comprehension, that is in the possession or custody of an agency or public official of this State or any of its political subdivisions, or is in the possession or custody of an association, the membership of which is composed exclusively of one or more of any of these entities, and has been received or prepared for use in connection with the transaction of public or governmental business or contains information relating to the transaction of public or governmental business," except as provided in the Maine Freedom of Access Act. *See* 1 M.R.S. § 402(3) & (3-A).

33. Purge. "Purge" means the act of rendering information unrecoverable in a storage space or to destroying information in a manner that it cannot be reconstituted.

a. There are many different strategies and techniques for information purging, which is often contrasted with information deletion (e.g., made inaccessible except to system administrators or other privileged users.)

34. Reasonably indicative. "Reasonably indicative" means an operational concept for documenting and sharing observed suspicious activity that takes into account:

a. The circumstances in which the observation of the activity is made that would cause a reasonable observer to be able to articulate a concern that the activity may indicate preoperational planning associated with terrorism or other criminal activity; and

b. The training and experience of the observer, including what, if any, training and experience the observer has as a law enforcement officer.

35. Right to Know. "Right to know" means a requirement for access to specific information to perform or assist in a lawful and authorized governmental function.

a. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity, or the roles and

responsibilities of particular personnel in the course of their official duties.

36. Regional Information Sharing Systems. Regional Information Sharing Systems ("RISS") means a national program of regionally-oriented services designed to enhance the ability of governmental criminal justice agencies to identify, target, and remove criminal conspiracies and activities spanning multi-jurisdictional, multi-State, and sometimes international boundaries; facilitate rapid exchange and sharing of information among the agencies pertaining to known or suspected criminals or criminal activity; and enhance coordination and communication among agencies that are in pursuit of criminal conspiracies determined to be inter-jurisdictional in nature.

    a. A MIAC ITS is not a RISS-maintained and -administered systems.

37. Source agency/organization. Defined in the Information Sharing Environment–Suspicious Activity Report ("ISE-SAR") Functional Standard 1.5.5, "source agency/organization" means the agency or organization that originates a SAR (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation).

    a. The source agency/organization originating a particular SAR will **always** be the source agency/organization for that particular SAR.

38. Submitting Agency/Organization. "Submitting Agency/Organization" means the organization that actuates the push of the Information Sharing Environment–Suspicious Activity Report ("ISE-SAR") to the Nationwide SAR Initiative ("NSI") community. The submitting organization and the source organization may be the same.
39. Suspicious Activity Report process. "Suspicious Activity Report process" ("SAR process") means the acquisition of information regarding behaviors and incidents related to crime and establishing a process to share that information to detect and prevent criminal activity, including, but not limited to, crime associated with terrorism.
40. Suspicious activity. "Suspicious activity" means observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.
41. Suspicious Activity Report information. "Suspicious Activity Report information" ("SAR information") means official documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity.

    a. SARs are a subset of tips and leads information.
    b. SAR information offers a standardized means for populating information repositories or data analysis tools.

c. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, the MIAC.

42. Terrorism information. Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), "terrorism information" means all information relating to:

a. The existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material 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.

43. Terrorism-related information. In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the Information Sharing Environment ("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. Such additional information may include intelligence information.

44. Tips and leads information. "Tips and leads information" means generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity.

a. Tips and leads information shall be maintained by the MIAC in a secure system, similar to information that rises to the level of reasonable suspicion.
b. 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.
c. Such information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful.

45. Users. "Users" means personnel from an external agency who are authorized to access, receive, and use MIAC information and intelligence databases for lawful purposes. Users are subject to the terms of use stated

on the MIAC Law Enforcement Secure Portal. For the purposes of this policy, "user" is the singular form of "users."

46. Validated Information. "Validated Information" means a tip or lead (including a Suspicious Activity Report) that has been reviewed and, when appropriate, combined with other information or further vetted and is determined to warrant additional action, such as investigation or dissemination, and/or maintenance as per the applicable record retention policy.

Appendix C

Fair Information Practice Principles

Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies within both government and the private sector.

Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into data privacy laws, policies, and governance documents around the world. For example, the core elements of the FIPPs can be found:

1. At the heart of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.[12]
2. Mirrored in many states' laws and in fusion centers' privacy policies.
3. In the ISO/IEC 29100 Privacy Framework, which has been adopted by numerous foreign countries and international organizations.

The following formulation of the FIPPs is used and implemented for the Information Sharing Environment (ISE) by the U.S. Department of Homeland Security (DHS).[13] Note, however, that under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or center policy.

A. **Purpose Specification**—Agencies should specifically articulate the authority that permits the collection of PII. The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes *compatible* with the original collection purpose).

   Implementing the Purpose Specification Principle—Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:

   1. Ensure that a valid lawful purpose exists and is documented for all collection of PII.
   2. Include the source and authority for the data so that access restrictions can be applied.
   3. Upon receipt of data containing PII from third parties, if possible, identify the purpose for which it was collected initially and limit agency use to only those uses compatible with the original purpose supporting collection.
   4. Ensure that metadata or other tags are associated with the data as it is shared.

[12] 5 U.S.C. § 552a.
[13] 6 U.S.C. § 142.

5. Institute a two-individual review and approval process to consider any Privacy Act or other legal or policy limitation before permitting use or sharing of data for purposes other than that for which it was collected.

B. **Data Quality/Integrity**—PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

Implementing the Data Quality/Integrity Principle—One important way to minimize potential downstream P/CRCL concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:

1. Properly labeling PII.
2. Determining a policy for safeguarding PII if there are "mixed" databases (i.e., those databases with PII on U.S. individuals and others, regardless of nationality).
3. Instituting a source verification procedure to ensure reporting is based only on authorized data.
4. Reconciling and updating PII whenever new relevant information is collected.
5. Developing a protocol for ensuring data corrections are passed to those entities with which information has been shared.
6. Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate or has been expunged.

C. **Collection Limitation/Data Minimization**—PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

Implementing the Collection Limitation/Data Minimization Principle—Collection limitation may be implemented by:

1. Designing a data storage system to pull data for review and then, if appropriate, automatically purging data after the specified retention period has been reached.
2. Limiting data field elements to only those that are relevant.
3. Ensuring that all distributed reports and products contain only that PII that is relevant and necessary (nothing extraneous or superfluous).
4. Ensuring that all shared information with PII meets required thresholds for sharing, such as reasonable suspicion.

D. **Use Limitation**—PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law.

Implementing the Use Limitation Principle—Sharing information should be tempered by adherence to key principles such as "authorized access." Use limitation may be implemented by:

1. Limiting users of data to those with credential-based access.
2. Requiring that justifications be entered and logs maintained for all queries with sensitive PII and that an internal review process of those logs takes place at specified intervals.
3. Requiring senior analysts to review all reports that use PII before dissemination to ensure (a) that PII is relevant and necessary and (b) that the recipient is authorized to receive the information in the performance of an authorized activity.
4. Prior to sharing information, verify that partners have a lawful purpose for requesting information.
5. Creating multiple use-based distribution lists and restricting distribution to those authorized to receive the information.

E. **Security/Safeguards**—Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

Implementing the Security/Safeguards Principle—This principle can be implemented by:

1. Maintaining up-to-date technology for network security.
2. Ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access is documented and auditable.
3. Ensuring that physical security measures are in place, such as requiring an identification card, credentials, and/or passcode for data access; disabling computers' USB ports; and implementing firewalls to prevent access to commercial e-mail or messaging services.
4. Implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period.
5. Ensuring that data system purge protocols include complete record deletion on all backup systems.
6. Transitioning older repositories into more modern systems to improve access controls.
7. Masking data so that it is viewable only to authorized users.
8. Maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals.
9. Requiring authorized users to sign nondisclosure agreements.

F. **Accountability/Audit**—Agency personnel and contractors are accountable for complying with measures implementing the FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

Implementing the Accountability/Audit Principle—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:

1. Ensuring that upon entry for duty, all staff take an oath to adhere to the privacy and civil liberties protections articulated in the center's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
2. Conducting effective orientation and periodic refresher training, including P/CRCL protections, for all individuals handling PII.
3. Tailoring training to specific job functions, database access, or data source/storage requirements.
4. Conducting regular audits of all systems in which records are kept to ensure compliance with the P/CRCL policies and all legal requirements.
5. Following a privacy incident handling procedure for any data breaches or policy violations.
6. Denying database access to individuals until they have completed mandatory systems access training (including training for handling of PII), show a mission need for access, and have any necessary clearances.
7. Developing targeted and consistent corrective actions whenever noncompliance is found.

G. **Openness/Transparency**—To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the P/CRCL policy, and contact information for data corrections and complaints.

Implementing the Openness/Transparency Principle—Agencies can implement the Openness/Transparency principle by:

1. Providing reports to an internal or external oversight body concerned with P/CRCL issues, including P/CRCL audit results.
2. Publishing the P/CRCL policy and redress procedures.
3. Meeting with community groups through initiatives or through other opportunities to explain the agency's mission and P/CRCL protections.
4. Responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public.
5. Conducting and publishing Privacy Impact Assessments (PIAs) in advance of implementing any new technologies that affect PII, thereby demonstrating that P/CRCL issues have been considered and addressed.

H. **Individual Participation**—To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use,

dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII.

Implementing the Individual Participation Principle—To the extent appropriate, agencies can implement the Individual Participation principle by:

1. Collecting information directly from the individual, to the extent possible and practical.
2. Providing the individual with the ability to find out whether an agency maintains a record relating to him or her and, if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial.
3. Putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.