Fall | 2010

BOSTON REGIONAL INTELLIGENCE CENTER

BRIC

Boston Regional Intelligence Center
Privacy, Civil Rights and Civil Liberties Protection Policy

The Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9111 Commission Act of 2007, established an information sharing environment for the sharing of terrorism-related information while protecting the privacy, civil rights, and civil liberties of individuals. The *Guidelines to Ensure that Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* ("ISE Privacy Guidelines") require relevant entities, including fusion centers, to have a written privacy protection policy in place that is "at least as comprehensive" as the ISE Privacy Guidelines.

This policy, produced by the Boston Regional Intelligence Center Privacy Committee, in collaboration with Boston Police Department's Office of the Legal Advisor, was reviewed and approved by the Department of Homeland Security Privacy and Civil Liberties Sub-Interagency Policy Committee on November 3, 2010 and was determined to be "at least as comprehensive" as the ISE Privacy Guidelines. The policy as implemented is intended to govern how the Boston Regional Intelligence Center will handle personally identifiable information and all other personal, sensitive information it seeks, receives and uses in the normal course of law enforcement, public safety and intelligence operations.

Superintendent Paul A. Fitzgerald
Bureau Chief, Bureau of Intelligence and Analysis

David N. Carabin
Director, Boston Regional Intelligence Center

Table of Contents

A. PURPOSE STATEMENT

The purpose of this privacy, civil rights, and civil liberties protection policy is to promote the Boston Regional Intelligence Center (hereafter "BRIC" or "the center") and user conduct that complies with applicable federal, state, local, and tribal law and assists the center and its participants in:

- Ensuring individual privacy, civil rights, civil liberties, and other protected interests;
- Increasing public safety and improving national security;
- Protecting the integrity of systems for the observation and reporting of terrorism-related criminal activity and information;
- Encouraging individuals or community groups to trust and cooperate with the justice system;
- Promoting governmental legitimacy and accountability; and
- Making the most effective use of public resources allocated to public safety agencies.

B. POLICY APPLICABILITY AND LEGAL COMPLIANCE

1. All BRIC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, agencies from which center information originates, and other authorized users will comply with:
    a. The center's privacy policy; and
    b. Applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. Constitution, the Massachusetts constitution, and applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to M.G.L. c. 4 §7, M.G.L. c. 6 §172, M.G.L. c. 12 §11H, M.G.L. c. 66 §10, and M.G.L. c. 66A §2, M.G.L. c. 151B, and 42 U.S.C.A. 1983.

    This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment [ISE] participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

2. The BRIC will provide a printed or electronic copy of this policy to all its personnel, nonagency personnel who provide services to the BRIC, and to each source agency and BRIC authorized user and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with applicable provisions of this policy.

3. The BRIC has adopted internal operating policies that are in compliance with the U.S. Constitution, the Massachusetts constitution, and applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to M.G.L. c. 4 §7, M.G.L. c. 6 §172, M.G.L. c. 12 §11H, M.G.L. c. 66 §10, and M.G.L. c. 66A §2, M.G.L. c. 151B, and 42 U.S.C.A. 1983.

C. GOVERNANCE AND OVERSIGHT

1. Primary responsibility for the operation of the BRIC; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Bureau Chief of the Boston Police Department's Bureau of Intelligence and Analysis and/or the Director of the BRIC.

2. The BRIC is guided by a designated privacy oversight committee. Members of the committee will be available to address questions and concerns regarding the BRIC's privacy policy, privacy and civil rights protections as provided in this policy, and the center's information gathering and collection, retention, and dissemination processes and procedures. The Committee will annually review and, as necessary, recommend updates to the policy in response to changes in law and implementation experience, including the results of internal reviews. The BRIC's privacy committee is guided by the BRIC's trained Privacy Officer, an individual having supervisory responsibilities within the BRIC as appointed by the Bureau Chief of the Boston Police Department's Bureau of Intelligence and Analysis and/or the Director of the BRIC. The Privacy Officer serves as the liaison for the Information Sharing Environment, overseeing implementation of and compliance with the Information Sharing Environment (ISE) Privacy Guidelines and ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.

3. The BRIC's Privacy Committee will be comprised of personnel with representatives appointed by the Bureau Chief of the Boston Police Department's Bureau of Intelligence and Analysis and/or the Director of the BRIC. The Privacy Committee shall consist of individuals both civilian and sworn law enforcement having supervisory responsibilities in (a) Homeland Security, (b) Criminal Intelligence, and (c) Legal Compliance. The Privacy Officer and the Privacy Committee can be contacted at the following address:

   Boston Regional Intelligence Center
   Boston Police Department
   Privacy Committee
   One Schroeder Plaza
   Boston, MA 02120
   (617) 343-4328

   The Privacy Committee receives reports regarding alleged errors and violations of the provisions of this policy, and receives and coordinates complaint resolution under the center's redress policy.

4. The BRIC's Privacy Committee ensures that enforcement procedures and sanctions outlined in Section N.3, Enforcement, are adequate and enforced.

D. TERMS AND DEFINITIONS

1. The primary terms and definitions used in this privacy policy are set forth in Appendix A, Terms and Definitions

E. INFORMATION

1. The BRIC will seek or retain information that:
   - Is based on a possible threat to public safety or the enforcement of the criminal law, or
   - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
   - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
   - Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
   - Based on the source agency's good faith belief, the information was acquired in accordance with agency policy and in a lawful manner.

   The BRIC may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads, subject to the policies and procedures specified in this policy.

   Please see Appendix C for the different types of information databases, systems, and records that the BRIC maintains or accesses and uses.

2. The BRIC will not seek or retain and originating agencies will agree to not submit information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientation.

3. The BRIC applies labels to agency-originated information to indicate to the accessing authorized user that:
   - The information is protected information as defined in Appendix A of policy and, to the extent expressly provided in this policy, includes organizational entities.
   - The information is subject to Massachusetts General Law and Federal Regulations restricting access, use, or disclosure.

4. The BRIC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) prior to retention to reflect the assessment, such as:
   - Whether the information consists of tips and leads data via formal email, phone, internet, or incident report submission, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.

- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
- The reliability of the source (for example, completely reliable, usually reliable, unreliable, unknown reliability).
- The validity of the content (for example, verified, unverified, and unable to verify).

5. At the time a decision is made by the BRIC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:
   - Protect confidential sources and police undercover techniques and methods.
   - Not interfere with or compromise pending criminal investigations.
   - Protect an individual's right of privacy or their civil rights and civil liberties.
   - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The labels assigned to existing information under Section E.5, above, will be reevaluated whenever:
   - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
   - There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

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

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

   - Store the information using the same storage method used for data that rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.

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

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

- Retain information for up to five (5) years in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" category (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition category.

- Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

8. The BRIC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

9. The BRIC will identify and review all protected information that may be accessed from or disseminated by the center prior to sharing that information. The BRIC will provide notice mechanisms, including but not limited to metadata or data field labels, that will enable authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The BRIC requires certain basic descriptive information labels to be entered and electronically associated with data or content for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
    - The name of the originating center, department or agency, component, and subcomponent.
    - The name of the center's justice information system from which the information is disseminated.
    - The date the information was collected and, where feasible, the date its accuracy was last verified.
    - The title and contact information for the person to whom questions regarding the information should be directed.

11. The BRIC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

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

F. ACQUIRING AND RECEIVING INFORMATION

1. Information acquisition and access, as well as investigative techniques used by the BRIC and source agencies, must comply with and adhere to applicable law, regulations and guidelines, including, but not limited to, M.G.L. c. 6 s. 172, M.G.L. c. 12 s. 11H, M.G.L. c. 41 s. 98, and M.G.L. c. 151B.
2. The BRIC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3. The BRIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.
4. Information-gathering and investigative techniques used by the BRIC will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.
5. External agencies that access the BRIC's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.
6. The BRIC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.
7. The BRIC will not directly or indirectly receive, seek, accept, or retain information from:
   - An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
   - An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

G. INFORMATION QUALITY ASSURANCE

1. The BRIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard [refer to Section I, Merging Records] has been met.
2. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence (verifiability, and reliability).
3. When errors and/or deficiencies are identified, the BRIC will correct the alleged errors and deficiencies or refer them to the originating agency, in a timely manner, and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.
4. The labeling of retained information will be reevaluated by the BRIC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.
5. The BRIC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when:
   a. The center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable;
   b. The center did not have authority to gather the information or to provide the information to another agency; or
   c. The center used prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

6. Originating agencies external to the BRIC are responsible for reviewing the quality and accuracy of the data provided to the center. When identified, the BRIC will notify the appropriate contact person in the originating agency, in writing or electronically if data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.
7. The BRIC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

H. COLLATION AND ANALYSIS

1. Information acquired or received by the BRIC or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.
2. Information subject to collation and analysis is information as defined and identified in [Refer to Section E, Information].
3. Information acquired or received by the BRIC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:
   - Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.
   - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.
4. At a minimum, all analytical products undergo peer review and, whenever practicable, a supervisory review prior to dissemination.

I. MERGING RECORDS

1. Records about an individual or organization from two or more sources will not be merged by the BRIC unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match.

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

J. SHARING AND DISCLOSURE

1. Credentialed, role-based access criteria will be used by the BRIC, as appropriate, to control:
   - The information to which a particular group or class of users can have access based on the group or class.
   - The information a class of users can add, change, delete, or print.
   - To whom, individually, the information can be disclosed and under what circumstances.
2. The BRIC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

3. Access to or disclosure of records retained by the BRIC will be provided only ***to persons within the center or in other governmental agencies*** who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the center.
4. Agencies external to the BRIC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information, unless otherwise marked.
5. Records retained by the BRIC may be accessed by or disseminated ***to those responsible for public protection, public safety, or public health*** only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.
6. Information gathered or collected and records retained by the BRIC may be accessed or disseminated ***for specific purposes*** upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center, the nature of the information requested, accessed, or received, and the specific purpose will be kept for no more than five years by the center.
7. Information gathered or collected and records retained by the BRIC may be accessed or disclosed ***to a member of the public*** only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.
8. Information gathered or collected and records retained by the BRIC ***will not*** be:
   - Sold, published, exchanged, or disclosed for commercial purposes.
   - Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
   - Disseminated to persons not authorized to access or use the information.

9. There are several categories of records that will ordinarily ***not be provided*** to the public. The following is not meant to be an exhaustive list, but serves as examples of records that will not be subject to public disclosure:

   - Records required to be kept confidential by law. (M.G.L. c. 4 s. 7(26)(a)
   - 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 accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
   - Investigatory records of law enforcement agencies. (M.L.G. c. 4 s. 7(26)(f).
   - A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism,

vulnerability assessments, risk planning documents, needs assessments, and threat assessments. (M.G.L. c. 4 s. 7(26)(n).
- Protected federal, state, local, or tribal records that were originated and controlled by another agency and were shared with the Department on the condition of confidentiality and non-disclosure.

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

K. REDRESS

K.1 DISCLOSURE

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

2. The existence, content, and source of the information will not be made available by the BRIC to an individual when:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (M.G.L. c. 4 s. 7(26)(f);
   - Disclosure would endanger the health or safety of an individual, organization, or community.
   - The information is in a criminal intelligence information system subject to 28 CFR Part 23 [see **28 CFR § 23.20(e)**].
   - Disclosure is not allowed by state and/or Federal law (M.G.L. c. 4 s. 7(26)(a);
   - The BRIC or user agency did not originate, or does not otherwise have a right to disclose, the information pursuant to a separate information sharing agreement. In such case, the BRIC or the user agency will refer the matter to the originating agency or the agency with a right to disclose the information; or
   - Any other production that would violate state and/or federal law, including but not limited to, M.G.L. c. 4 s. 7, M.G.L. c. 6 s. 172, or M.G.L. c. 66 s. 10.

K.2 CORRECTIONS

1. If an individual requests correction of information ***originating with the BRIC*** that has been disclosed, the center's Privacy Officer, on behalf of the Privacy Committee, will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

K.3 APPEALS

1. The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the Privacy Committee. The individual will also be informed of the procedure for appeal when the center or originating agency

has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

K.4 COMPLAINTS

1. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:
   (a) Is exempt from disclosure,
   (b) Has been or may be shared through the ISE, or
   (c) (1) Is held by the BRIC and
   (2) Allegedly has resulted in demonstrable harm to the complainant.

   The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer, on behalf of the Privacy Committee, at the following address:

   Boston Regional Intelligence Center
   Boston Police Department
   Privacy Committee
   One Schroeder Plaza
   Boston, MA 02120

   The Privacy Officer, on behalf of the Privacy Committee, will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer, on behalf of the Privacy Committee, will notify the originating agency in writing or electronically within ten (10) business days of the receipt of the complaint and, upon request, may assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within thirty (30) days and confirmed or corrected/purged if determined to be inaccurate, incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within thirty (30) days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

2. For the purposes of complaints, the BRIC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared to delineate protected information shared through the ISE from other data.

L. SECURITY SAFEGUARDS

1. The Bureau Chief of the Boston Police Department's Bureau of Intelligence and Analysis and/or the Director of the BRIC will designate a trained law enforcement supervisor assigned to serve as the center's Security Officer.
2. The BRIC will operate in a secure facility protected from external intrusion. The center will utilize secure internal and external safeguards against network intrusions. Access to the center's databases from outside the facility will be allowed only over secure networks.
3. The BRIC will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.
4. The BRIC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

5. Access to BRIC information will be granted only to center personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.
6. Queries made to the BRIC's data applications will be logged into the data system identifying the user initiating the query.
7. The BRIC will utilize watch logs to maintain audit trails of requested and disseminated information.
8. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.
9. The BRIC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.
10. The BRIC will immediately notify the originating agency from which the center received personal information of a suspected or confirmed breach of such information.

M. INFORMATION RETENTION AND DESTRUCTION

1. All applicable information will be reviewed for record retention (validation or purge) by BRIC at least every five (5) years, as provided by 28 CFR Part 23. The BRIC conducts quarterly reviews and ongoing maintenance to validate or purge information.
2. When information has no further value or meets the criteria for removal according to the BRIC's retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.
3. The BRIC will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.
4. No approval will be required from the originating agency before information held by the BRIC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.
5. Notification of proposed destruction or return of records may or may not be provided to the originating agency by the BRIC, depending on the relevance of the information and any agreement with the originating agency.
6. The BRIC keeps a record of dates when information is to be removed (purged) if not validated prior to the end of its period. An auto-generated notification is given prior to removal to prompt center personnel that a record is due for review and validation or purge.

N. ACCOUNTABILITY AND ENFORCEMENT

N.1 INFORMATION SYSTEM TRANSPARENCY

1. The BRIC will be open with the public in regard to information and intelligence collection practices. The center's privacy policy will be provided to the public for review, made available upon request, and posted to http://www.bpdnews.com.
2. The BRIC's Privacy Officer, on behalf of the Privacy Committee, will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections

in the information system(s) maintained or accessed by the center. The Privacy Committee can be contacted at:

Boston Regional Intelligence Center
Boston Police Department
Privacy Committee
One Schroeder Plaza
Boston, MA 02120
(617) 343-4328

N.2 ACCOUNTABILITY

1. The audit log of queries made to the BRIC will identify the user initiating the query.
2. The BRIC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for not more than five years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.
3. The BRIC follows agency-based user agreements for access to computer networks and systems. The BRIC will provide annual center-based personnel training to reinforce applicable laws and policies. The BRIC will adopt and implement procedures to evaluate the compliance of users with this policy and with applicable law, to include a review of logging access to BRIC information systems and periodic auditing of user compliance. These audits will be conducted at least annually and a record of the audits will be maintained by the Privacy Officer on behalf of the Privacy Committee.
4. The BRIC's personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Committee. See Section C.3.
5. The BRIC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by the center's Privacy Committee. This committee has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).
6. The BRIC's Privacy Committee will review the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and recommend updates, as needed, to the BRIC Director in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

N.3 ENFORCEMENT

1. If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Bureau Chief of the Boston Police Department's Bureau of Intelligence and Analysis and/or the Director of the BRIC may:
   - Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
   - Apply administrative and/or legal actions or sanctions as consistent with department rules and regulations, applicable law, or as provided in agency/center personnel policies.
   - If the authorized user is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.

2. The BRIC reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the center's privacy policy.

O. TRAINING

1. The BRIC will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy prior to granting access:
   - All assigned personnel of the center.
   - Personnel providing information technology services to the center.
   - Staff in other public agencies or private contractors providing services to the center.
   - Users who are not employed by the center or a contractor.
2. The BRIC will provide special training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.
3. The BRIC's privacy policy training program will cover:
   - Purposes of the privacy, civil rights, and civil liberties protection policy.
   - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the center.
   - Originating and participating agency responsibilities and obligations under applicable law and policy.
   - How to implement the policy in the day-to-day work of the user, whether a paper or systems user.
   - The impact of improper activities associated with infractions within or through the agency.
   - Mechanisms for reporting violations of center privacy protection policies and procedures.
   - The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

APPENDIX A: TERMS AND DEFINITIONS

The following is a list of primary terms and definitions used throughout this policy.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

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

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

Agency—The Boston Regional Intelligence Center (BRIC) and all agencies that access, contribute, and share information in the BRIC's justice information systems.

Audit Trail—Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

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

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

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

Center—Center refers to the Boston Regional Intelligence Center (BRIC) and all participating agencies.

Civil Liberties—Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government

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

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

Confidentiality—Confidentiality refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

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

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Data—Elements of information.

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media such as computer tapes, hard drives, or laptop computers containing such media upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

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

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

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

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

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

The eight FIPs are:
1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

General Information or Data—Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Urban Area Fusion Center— A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity

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

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family

name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

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

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

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

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

Intelligence-Led Policing (ILP)—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

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

ISE-SAR—A suspicious activity report (SAR) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

ISE-SAR Information Exchange Package Documentation (IEPD) —A schema that facilitates the posting and sharing of ISE-SAR information. The ISE-SAR IEPD is used to represent ISE information in two different data formats:

(1) The **Detailed format** includes information contained in all data elements set forth in Section IV of the ISE-SAR FS ("ISE-SAR Exchange Data Model"), including fields denoted as privacy fields.

(2) The **Summary format** excludes certain privacy fields as identified in the ISE-SAR FS. The ISE-SAR FS identifies the minimum privacy fields that must be excluded. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with applicable legal requirements.

Label—Marking(s) applied to disseminated information and products with indications to the accessing authorized user indicating that the information is protected information, including organizational entities,

and the information is subject to Massachusetts General Law and Federal Regulations restricting access, use, or disclosure.

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

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

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

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

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

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

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

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

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

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

Participating Agencies—Participating agencies, for purposes of the EE Initiative, include source [the agency or entity that originates SAR (and, when authorized, ISE-SAR) information], submitting (which is the agency or entity posting ISE-SAR information to the shared space), and user (which is an agency or entity authorized by the submitting agency or other authorized agency or entity, to access ISE-SAR information, including information in the shared space(s), and which may include analytical or operational component(s) of the submitting or authorizing agency or entity) agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

Personal Information— Information which can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

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

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons—Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

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

Privacy fields—Data fields in ISE-SAR IEPD's that contain personal information.

Privacy Policy—A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information

collection, analysis, maintenance, disclosure, and access. The purpose of the privacy policy is to articulate that the center will adhere to those legal requirements and center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

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

Protected Information— Protected information includes personal information about any individual that is subject to information privacy or other protections by law, including the U.S. Constitution, the Massachusetts constitution, and other applicable law.

Public—Public includes:

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

Public does not include:

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

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

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

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

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

Retention—See Storage.

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

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

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

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

Shared Space—A networked data and information repository that is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

Sharing—refers to the act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

Source Agency—Source agency refers to the agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Submitting Agency—Submitting agency refers to the agency or entity providing ISE-SAR information to the shared space)

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

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

Terrorism Information—Consistent with Section 1016(a)(4) of IRTPA, all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism, (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations, (c) communications of or by such groups or individuals, or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information—In accordance with IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also Information Sharing Environment Implementation Plan (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information" (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

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

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

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

User Agency—User agency refers to the agency or entity authorized by the submitting agency, or other authorized agency or entity, to access ISE-SAR information in the shared space(s), and which may include analytical or operational component(s) of the submitting or authorizing agency or entity.

APPENDIX B: APPLICABLE LEGAL REFERENCES

Effective: October 31, 2007
Massachusetts General Laws Annotated Currentness
Part I. Administration of the Government (Ch. 1-182)
Title X. Public Records (Ch. 66-66A)
Chapter 66A. Fair Information Practices (Refs & Annos)

§ 2. Holders maintaining personal data system; duties
Every holder maintaining personal data shall:--
(a) identify one individual immediately responsible for the personal data system who shall insure that the requirements of this chapter for preventing access to or dissemination of personal data are followed;
(b) inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the personal data system, or the use of any personal data contained therein, of each safeguard required by this chapter, of each rule and regulation promulgated pursuant to section three which pertains to the operation of the personal data system, and of the civil remedies described in section three B of chapter two hundred and fourteen available to individuals whose rights under chapter sixty-six A are allegedly violated;
(c) not allow any other agency or individual not employed by the holder to have access to personal data unless such access is authorized by statute or regulations which are consistent with the purposes of this chapter or is approved by the data subject whose personal data are sought if the data subject is entitled to access under clause
(i). Medical or psychiatric data may be made available to a physician treating a data subject upon the request of said physician, if a medical or psychiatric emergency arises which precludes the data subject's giving approval for the release of such data, but the data subject shall be given notice of such access upon termination of the emergency. A holder shall provide lists of names and addresses of applicants for professional licenses and lists of professional licensees to associations or educational organizations recognized by the appropriate professional licensing or examination board. A holder shall comply with a data subject's request to disseminate his data to a third person if practicable and upon payment, if necessary, of a reasonable fee; provided, however, that nothing in this section shall be construed to prohibit disclosure to or access by the bureau of special investigations to the records or files of the department of transitional assistance for the purposes of fraud detection and control;
(d) take reasonable precautions to protect personal data from dangers of fire, identity theft, theft, flood, natural disaster, or other physical threat;
(e) comply with the notice requirements set forth in section sixty-three of chapter thirty;
(f) in the case of data held in automated personal data systems, and to the extent feasible with data held in manual personal data systems, maintain a complete and accurate record of every access to and every use of any personal data by persons or organizations outside of or other than the holder of the data, including the identity of all such persons and organizations which have gained access to the personal data and their intended use of such data and the holder need not record any such access of its employees acting within their official duties;
(g) to the extent that such material is maintained pursuant to this section, make available to a data subject upon his request in a form comprehensible to him, a list of the uses made of his personal data, including the identity of all persons and organizations which have gained access to the data;
(h) maintain personal data with such accuracy, completeness, timeliness, pertinence and relevance as is necessary to assure fair determination of a data subject's qualifications, character, rights, opportunities, or benefits when such determinations are based upon such data;

(i) inform in writing an individual, upon his request, whether he is a data subject, and if so, make such data fully available to him or his authorized representative, upon his request, in a form comprehensible to him, unless doing so is prohibited by this clause or any other statute. A holder may withhold from a data subject for the period hereinafter set forth, information which is currently the subject of an investigation and the disclosure of which would probably so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest, but this sentence is not intended in any way to derogate from any right or power of access the data subject might have under administrative or judicial discovery procedures. Such information may be withheld for the time it takes for the holder to complete its investigation and commence an administrative or judicial proceeding on its basis, or one year from the commencement of the investigation or whichever occurs first. In making any disclosure of information to a data subject pursuant to this chapter the holder may remove personal identifiers relating to a third person, except where such third person is an officer or employee of government acting as such and the data subject is not. No holder shall rely on any exception contained in clause Twentysixth of section seven of chapter four to withhold from any data subject personal data otherwise accessible to him under this chapter;
(j) establish procedures that (1) allow each data subject or his duly authorized representative to contest the accuracy, completeness, pertinence, timeliness, relevance or dissemination of his personal data or the denial of access to such data maintained in the personal data system and (2) permit personal data to be corrected or amended when the data subject or his duly authorized representative so requests and there is no disagreement concerning the change to be made or, when there is disagreement with the data subject as to whether a change should be made, assure that the data subject's claim is noted and included as part of the data subject's personal data and included in any subsequent disclosure or dissemination of the disputed data;
(k) maintain procedures to ensure that no personal data are made available in response to a demand for data made by means of compulsory legal process, unless the data subject has been notified of such demand in reasonable time that he may seek to have the process quashed;
(l) not collect or maintain more personal data than are reasonably necessary for the performance of the holder's statutory functions.
M.G.L.A. 66A § 2 Page 2

CREDIT(S)
Added by St.1975, c. 776, § 1. Amended by St.1976, c. 249, § 2; St.1977, c. 691, §§ 7 to 12; St.1995, c. 5, § 34;
St.2007, c. 82, § 2, eff. Oct. 31, 2007.
Current through Chapter 10 of the 2009 1st Annual Sess.

Effective: December 13, 2003
United States Code Annotated Currentness
Title 6. Domestic Security (Refs & Annos)
Chapter 1. Homeland Security Organization
Subchapter VIII. Coordination with Non-Federal Entities; Inspector General; United States Secret Service;
Coast Guard; General Provisions
Part I. Information Sharing

§ 482. Facilitating homeland security information sharing procedures
(a) Procedures for determining extent of sharing of homeland security information
(1) The President shall prescribe and implement procedures under which relevant Federal agencies--
(A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;
(B) identify and safeguard homeland security information that is sensitive but unclassified; and

(C) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.
(2) The President shall ensure that such procedures apply to all agencies of the Federal Government.
(3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.
(4) Such procedures shall not change the requirements and authorities to protect sources and methods.
(b) Procedures for sharing of homeland security information
(1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection (a) of this section, together with assessments of the credibility of such information.
(2) Each information sharing system through which information is shared under paragraph (1) shall--
(A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;
(B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information;
(C) be configured to allow the efficient and effective sharing of information; and
(D) be accessible to appropriate State and local personnel.
(3) The procedures prescribed under paragraph (1) shall establish conditions on the use of information shared under paragraph (1)--
(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;
(B) to ensure the security and confidentiality of such information;
(C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and
(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.
(4) The procedures prescribed under paragraph (1) shall ensure, to the greatest extent practicable, that the information sharing system through which information is shared under such paragraph include existing information sharing systems, including, but not limited to, the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation.
(5) Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph (1), and shall therefore have access to all information, as appropriate, shared under such paragraph.
(6) The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use such information sharing systems--
(A) to access information shared with such personnel; and
(B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.
(7) Under procedures prescribed jointly by the Director of Central Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph (6) and integrate such information with existing intelligence.
(c) Sharing of classified information and sensitive but unclassified information with State and local personnel
(1) The President shall prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security

information that remains classified or otherwise protected after the determinations prescribed under the procedures set forth in subsection (a) of this section.
(2) It is the sense of Congress that such procedures may include 1 or more of the following means:
(A) Carrying out security clearance investigations with respect to appropriate State and local personnel.
(B) With respect to information that is sensitive but unclassified, entering into nondisclosure agreements with appropriate State and local personnel.
(C) Increased use of information-sharing partnerships that include appropriate State and local personnel, such as the Joint Terrorism Task Forces of the Federal Bureau of Investigation, the Anti-Terrorism Task Forces of the Department of Justice, and regional Terrorism Early Warning Groups.
(3)(A) The Secretary shall establish a program to provide appropriate training to officials described in subparagraph
(B) in order to assist such officials in--
(i) identifying sources of potential terrorist threats through such methods as the Secretary determines appropriate;
(ii) reporting information relating to such potential terrorist threats to the appropriate Federal agencies in the appropriate form and manner;
(iii) assuring that all reported information is systematically submitted to and passed on by the Department for use by appropriate Federal agencies; and
(iv) understanding the mission and roles of the intelligence community to promote more effective information sharing among Federal, State, and local officials and representatives of the private sector to prevent terrorist attacks against the United States.
(B) The officials referred to in subparagraph (A) are officials of State and local government agencies and representatives of private sector entities with responsibilities relating to the oversight and management of first responders, counterterrorism activities, or critical infrastructure.
(C) The Secretary shall consult with the Attorney General to ensure that the training program established in subparagraph (A) does not duplicate the training program established in section 908 of the USA PATRIOT Act (Public Law 107-56; 28 U.S.C. 509 note).
(D) The Secretary shall carry out this paragraph in consultation with the Director of Central Intelligence and the Attorney General.
(d) Responsible officials
For each affected Federal agency, the head of such agency shall designate an official to administer this chapter with respect to such agency.
(e) Federal control of information
Under procedures prescribed under this section, information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information.
(f) Definitions
As used in this section:
(1) The term “homeland security information” means any information possessed by a Federal, State, or local agency that--
(A) relates to the threat of terrorist activity;
(B) relates to the ability to prevent, interdict, or disrupt terrorist activity;
(C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or
(D) would improve the response to a terrorist act.
(2) The term “intelligence community” has the meaning given such term in section 401a(4) of Title 50.
(3) The term “State and local personnel” means any of the following persons involved in prevention, preparation, or response for terrorist attack:
(A) State Governors, mayors, and other locally elected officials.
(B) State and local law enforcement personnel and firefighters.
(C) Public health and medical professionals.

(D) Regional, State, and local emergency management agency personnel, including State adjutant generals.
(E) Other appropriate emergency response agency personnel.
(F) Employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section.
(4) The term “State” includes the District of Columbia and any commonwealth, territory, or possession of the United States.
(g) Construction
Nothing in this chapter shall be construed as authorizing any department, bureau, agency, officer, or employee of the Federal Government to request, receive, or transmit to any other Government entity or personnel, or transmit to any State or local entity or personnel otherwise authorized by this chapter to receive homeland security information, any information collected by the Federal Government solely for statistical purposes in violation of any other provision of law relating to the confidentiality of such information.
CREDIT(S)
6 U.S.C.A. § 482 Page 4

(Pub.L. 107-296, Title VIII, § 892, Nov. 25, 2002, 116 Stat. 2253; Pub.L. 108-177, Title III, § 316(a), Dec. 13, 2003, 117 Stat. 2610.)
2002 Acts. This section effective 60 days after Nov. 25, 2002, see Pub.L. 107-296, § 4, set out as a note under 6 U.S.C.A. § 101.
Current through P.L. 111-15 (excluding P.L. 111-11 and 111-13) approved 4-24-09

END OF DOCUMENT
6 U.S.C.A. § 482 Page 5

Effective: March 30, 2009
Massachusetts General Laws Annotated Currentness
Part I. Administration of the Government (Ch. 1-182)
Title I. Jurisdiction and Emblems of the Commonwealth, the General Court, Statutes and Public Documents
(Ch. 1-5)
Chapter 4. Statutes (Refs & Annos)

§ 7. Definitions of statutory terms; statutory construction
In construing statutes the following words shall have the meanings herein given, unless a contrary intention clearly appears:
First, “Aldermen”, “board of aldermen”, “mayor and aldermen”, “city council” or “mayor” shall, in a city which has no such body or officer, mean the board or officer having like powers or duties.
Second, “Annual meeting”, when applied to towns, shall mean the annual meeting required by law to be held in the month of February, March or April.
Second A, “Appointing authority”, when used in connection with the operation of municipal governments shall include the mayor of a city and the board of selectmen of a town unless some other local office is designated as the appointing authority under the provisions of a local charter.
Third, “Assessor” shall include any person chosen or appointed in accordance with law to perform the duties of an assessor.
Third A, “Board of selectmen”, when used in connection with the operation of municipal governments shall include any other local office which is performing the duties of a board of selectmen, in whole or in part, under the provisions of a local charter.
<[There is no clause Fourth.]>

Fifth, “Charter”, when used in connection with the operation of city and town government shall include a written instrument adopted, amended or revised pursuant to the provisions of chapter forty-three B which establishes and defines the structure of city and town government for a particular community and which may create local offices, and distribute powers, duties and responsibilities among local offices and which may establish and define certain procedures to be followed by the city or town government. Special laws enacted by the general court applicable only to one city or town shall be deemed to have the force of a charter and may be amended, repealed and revised in accordance with the provisions of chapter forty-three B unless any such special law contains a specific prohibition against such action.
Fifth A, “Chief administrative officer”, when used in connection with the operation of municipal governments, shall include the mayor of a city and the board of selectmen in a town unless some other local office is designated to be the chief administrative officer under the provisions of a local charter.
Fifth B, “Chief executive officer”, when used in connection with the operation of municipal governments shall include the mayor in a city and the board of selectmen in a town unless some other municipal office is designated to be the chief executive officer under the provisions of a local charter.
Sixth, “City solicitor” shall include the head of the legal department of a city or town.
Sixth A, “Coterminous”, shall mean, when applied to the term of office of a person appointed by the governor, the period from the date of appointment and qualification to the end of the term of said governor; provided that such person shall serve until his successor is appointed and qualified; and provided, further, that the governor may remove such person at any time, subject however to the condition that if such person receives notice of the termination of his appointment he shall have the right, at his request, to a hearing within thirty days from receipt of such notice at which hearing the governor shall show cause for such removal, and that during the period following receipt of such notice and until final determination said person shall receive his usual compensation but shall be deemed suspended from his office.
Seventh, “District”, when applied to courts or the justices or other officials thereof, shall include municipal.
Eighth, “Dukes”, “Dukes county” or “county of Dukes” shall mean the county of Dukes county.
Ninth, “Fiscal year”, when used with reference to any of the offices, departments, boards, commissions, institutions or undertakings of the commonwealth, shall mean the year beginning with July first and ending with the following June thirtieth.
Tenth, “Gaming”, “illegal gaming” or “unlawful gaming” shall include every act punishable under any law relative to lotteries, policy lotteries or policy, the buying and selling of pools or registering of bets.
Eleventh, “Grantor” may include every person from or by whom a freehold estate or interest passes in or by any deed; and “grantee” may include every person to whom such estate or interest so passes.
Twelfth, “Highway”, “townway”, “public way” or “way” shall include a bridge which is a part thereof.
Thirteenth, “In books”, when used relative to the records of cities and towns, shall not prohibit the making of such records on separate leaves, if such leaves are bound in a permanent book upon the completion of a sufficient number of them to make an ordinary volume.
Fourteenth, “Inhabitant” may mean a resident in any city or town.
<[There is no clause Fifteenth.]>
Sixteenth, “Issue”, as applied to the descent of estates, shall include all the lawful lineal descendants of the ancestor.
Seventeenth, “Land”, “lands” and “real estate” shall include lands, tenements and hereditaments, and all rights thereto and interests therein; and “recorded”, as applied to plans, deeds or other instruments affecting land, shall, as affecting registered land, mean filed and registered.
Eighteenth, “Legal holiday” shall include January first, July fourth, November eleventh, and Christmas Day, or the day following when any of said days occurs on Sunday, and the third Monday in January, the third Monday in February, the third Monday in April, the last Monday in May, the first Monday in September, the second Monday in October, and Thanksgiving Day. “Legal holiday” shall also include, with respect to Suffolk county only, March seventeenth and June seventeenth, or the day following when said days occur on Sunday; provided, however, that the words “legal holiday” as used in section

forty-five of chapter one hundred and forty-nine shall not include March seventeenth, or the day following when said day occurs on Sunday.

Eighteenth A, “Commemoration day” shall include March fifteenth, in honor of Peter Francisco day, May twentieth, in honor of General Marquis de Lafayette and May twenty-ninth, in honor of the birthday of President John F. Kennedy. The governor shall issue a proclamation in connection with each such commemoration day.

Eighteenth B, “Legislative body”, when used in connection with the operation of municipal governments shall include that agency of the municipal government which is empowered to enact ordinances or by-laws, adopt an annual budget and other spending authorizations, loan orders, bond authorizations and other financial matters and whether styled a city council, board of aldermen, town council, town meeting or by any other title.

Nineteenth, “Month” shall mean a calendar month, except that, when used in a statute providing for punishment by imprisonment, one “month” or a multiple thereof shall mean a period of thirty days or the corresponding multiple thereof; and “year”, a calendar year.

Nineteenth A, “Municipality” shall mean a city or town.

Twentieth, “Net indebtedness” shall mean the indebtedness of a county, city, town or district, omitting debts created for supplying the inhabitants with water and other debts exempted from the operation of the law limiting their indebtedness, and deducting the amount of sinking funds available for the payment of the indebtedness included.

Twenty-first, “Oath” shall include affirmation in cases where by law an affirmation may be substituted for an oath.

Twenty-second, “Ordinance”, as applied to cities, shall be synonymous with by-law.

Twenty-third, “Person” or “whoever” shall include corporations, societies, associations and partnerships. Twenty-fourth, “Place” may mean a city or town.

Twenty-fifth, “Preceding” or “following”, used with reference to any section of the statutes, shall mean the section last preceding or next following, unless some other section is expressly designated in such reference.

Twenty-sixth, “Public records” shall mean all books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any officer or employee of any agency, executive office, department, board, commission,

bureau, division or authority of the commonwealth, or of any political subdivision thereof, or of any authority established by the general court to serve a public purpose, unless such materials or data fall within the following exemptions in that they are:

(a) specifically or by necessary implication exempted from disclosure by statute;

(b) related solely to internal personnel rules and practices of the government unit, provided however, that such records shall be withheld only to the extent that proper performance of necessary governmental functions requires such withholding;

(c) personnel and medical files or information; also any other materials or data relating to a specifically named individual, the disclosure of which may constitute an unwarranted invasion of personal privacy;

(d) inter-agency or intra-agency memoranda or letters relating to policy positions being developed by the agency; but this subclause shall not apply to reasonably completed factual studies or reports on which the development of such policy positions has been or may be based;

(e) notebooks and other materials prepared by an employee of the commonwealth which are personal to him and not maintained as part of the files of the governmental unit;

(f) investigatory materials necessarily compiled out of the public view by law enforcement or other investigatory officials the disclosure of which materials would probably so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest;

(g) trade secrets or commercial or financial information voluntarily provided to an agency for use in developing governmental policy and upon a promise of confidentiality; but this subclause shall not apply to information submitted as required by law or as a condition of receiving a governmental contract or other benefit;

(h) proposals and bids to enter into any contract or agreement until the time for the opening of bids in the case of proposals or bids to be opened publicly, and until the time for the receipt of bids or proposals has expired in all other cases; and inter-agency or intra-agency communications made in connection with an evaluation process for reviewing bids or proposals, prior to a decision to enter into negotiations with or to award a contract to, a particular person;
(i) appraisals of real property acquired or to be acquired until (1) a final agreement is entered into; or (2) any litigation relative to such appraisal has been terminated; or (3) the time within which to commence such litigation has expired;
(j) the names and addresses of any persons contained in, or referred to in, any applications for any licenses to carry or possess firearms issued pursuant to chapter one hundred and forty or any firearms identification cards issued pursuant to said chapter one hundred and forty and the names and addresses on sales or transfers of any firearms, rifles, shotguns, or machine guns or ammunition therefor, as defined in said chapter one hundred and forty and the names and addresses on said licenses or cards;
<[There is no subclause (k).]>
(l) questions and answers, scoring keys and sheets and other materials used to develop, administer or score a test, examination or assessment instrument; provided, however, that such materials are intended to be used for another test, examination or assessment instrument;
(m) contracts for hospital or related health care services between (i) any hospital, clinic or other health care facility operated by a unit of state, county or municipal government and (ii) a health maintenance organization arrangement approved under chapter one hundred and seventy-six I, a nonprofit hospital service corporation or medical service corporation organized pursuant to chapter one hundred and seventy-six A and chapter one hundred and seventy-six B, respectively, a health insurance corporation licensed under chapter one hundred and seventy-five or any legal entity that is self insured and provides health care benefits to its employees.
(n) records, including, but not limited to, blueprints, plans, policies, procedures and schematic drawings, which relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, or any other records relating to the security or safety of persons or buildings, structures, facilities, utilities, transportation or other infrastructure located within the commonwealth, the disclosure of which, in the reasonable judgment of the record custodian, subject to review by the supervisor of public records under subsection (b) of section 10 of chapter 66, is likely to jeopardize public safety.
(o) the home address and home telephone number of an employee of the judicial branch, an unelected employee of the general court, an agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or of a political subdivision thereof or of an authority established by the general court to serve a public purpose, in the custody of a government agency which maintains records identifying persons as falling within those categories; provided that the information may be disclosed to an employee organization under chapter 150E, a nonprofit organization for retired public employees under chapter 180, or a criminal justice agency as defined in section 167 of chapter 6.
(p) the name, home address and home telephone number of a family member of a commonwealth employee, contained in a record in the custody of a government agency which maintains records identifying persons as falling within the categories listed in subclause (o).
(q) Adoption contact information and indices therefore of the adoption contact registry established by section 31 of chapter 46.
(r) Information and records acquired under chapter 18C by the office of the child advocate.
(s) trade secrets or confidential, competitively-sensitive or other proprietary information provided in the course of activities conducted by a governmental body as an energy supplier under a license granted by the department of public utilities pursuant to section 1F of chapter 164, in the course of activities conducted as a municipal aggregator under section 134 of said chapter 164 or in the course of activities conducted by a cooperative consisting of governmental entities organized pursuant to section 136 of said chapter 164, when such governmental body, municipal aggregator or cooperative determines that

such disclosure will adversely affect its ability to conduct business in relation to other entities making, selling or distributing electric power and energy; provided, however, that this subclause shall not exempt a public entity from disclosure required of a private entity so licensed. Any person denied access to public records may pursue the remedy provided for in section ten of chapter sixtysix.
Twenty-seventh, “Salary” shall mean annual salary.
Twenty-eighth, “Savings banks” shall include institutions for savings.
<[There is no clause Twenty-ninth.]>
Thirtieth, “Spendthrift” shall mean a person who is liable to be put under guardianship on account of excessive drinking, gaming, idleness or debauchery.
Thirty-first, “State”, when applied to the different parts of the United States, shall extend to and include the District of Columbia and the several territories; and the words “United States” shall include said district and territories.
Thirty-second, “State auditor” and “state secretary” shall mean respectively the auditor of the commonwealth and the secretary of the commonwealth. “State treasurer” or “treasurer of the commonwealth” shall mean the treasurer and receiver general as used in the constitution of the commonwealth, and shall have the same meaning in all contracts, instruments, securities and other documents. Thirty-third, “Swear” shall include affirm in cases in which an affirmation may be substituted for an oath. When applied to public officers who are required by the constitution to take oaths therein prescribed, it shall refer to those oaths; and when applied to any other officer it shall mean sworn to the faithful performance of his official duties.
Thirty-fourth, “Town”, when applied to towns or officers or employees thereof, shall include city.
Thirty-fifth, “Valuation”, as applied to a town, shall mean the valuation of such town as determined by the last preceding apportionment made for the purposes of the state tax.
Thirty-sixth, “Water district” shall include water supply district.
Thirty-seventh, “Will” shall include codicils.
Thirty-eighth, “Written” and “in writing” shall include printing, engraving, lithographing and any other mode of representing words and letters; but if the written signature of a person is required by law, it shall always be his own handwriting or, if he is unable to write, his mark.
Thirty-ninth, “Annual election”, as applied to municipal elections in cities holding such elections biennially, shall mean biennial election.
Fortieth, “Surety” or “Sureties”, when used with reference to a fidelity bond of an officer or employee of a county, city, town or district, shall mean a surety company authorized to transact business in the commonwealth.
Forty-first, “Population”, when used in connection with the number of inhabitants of a county, city, town or district, shall mean the population as determined by the last preceding national census.
<[There is no clause Forty-second.]>
Forty-third, “Veteran” shall mean (1) any person, (a) whose last discharge or release from his wartime service as defined herein, was under honorable conditions and who (b) served in the army, navy, marine corps, coast guard, or air force of the United States, or on full time national guard duty under Titles 10 or 32 of the United States Code or under sections 38, 40 and 41 of chapter 33 for not less than 90 days active service, at least 1 day of which was for wartime service; provided, however, than any person who so served in wartime and was awarded a service-connected disability or a Purple Heart, or who died in such service under conditions other than dishonorable, shall be deemed to be a veteran notwithstanding his failure to complete 90 days of active service; (2) a member of the American Merchant Marine who served in armed conflict between December 7, 1941 and December 31, 1946, and who has received honorable discharges from the United States Coast Guard, Army, or Navy; (3) any person (a) whose last discharge from active service was under honorable conditions, and who (b) served in the army, navy, marine corps, coast guard, or air force of the United States for not less than 180 days active service; provided, however, that any person who so served and was awarded a service-connected disability or who died in such service under conditions other than dishonorable, shall be deemed to be a veteran notwithstanding his failure to complete 180 days of active service.
“Wartime service” shall mean service performed by a “Spanish War veteran”, a “World War I veteran”, a

“World War II veteran”, a “Korean veteran”, a “Vietnam veteran”, a “Lebanese peace keeping force veteran”, a “Grenada rescue mission veteran”, a “Panamanian intervention force veteran”, a “Persian Gulf veteran”, or a member of the “WAAC” as defined in this clause during any of the periods of time described herein or for which such medals described below are awarded.

“Spanish War veteran” shall mean any veteran who performed such wartime service between February fifteenth, eighteen hundred and ninety-eight and July fourth, nineteen hundred and two.

“World War I veteran” shall mean any veteran who (a) performed such wartime service between April sixth, nineteen hundred and seventeen and November eleventh, nineteen hundred and eighteen, or (b) has been awarded the World War I Victory Medal, or (c) performed such service between March twenty-fifth, nineteen hundred and seventeen and August fifth, nineteen hundred and seventeen, as a Massachusetts National Guardsman. “World War II veteran” shall mean any veteran who performed such wartime service between September 16, 1940 and July 25, 1947, and was awarded a World War II Victory Medal, except that for the purposes of chapter 31 it shall mean all active service between the dates of September 16, 1940 and June 25, 1950. “Korean veteran” shall mean any veteran who performed such wartime service between June twenty-fifth, nineteen hundred and fifty and January thirty-first, nineteen hundred and fifty-five, both dates inclusive, and any person who has received the Korea Defense Service Medal as established in the Bob Stump National Defense Authorization Act for fiscal year 2003.

“Korean emergency” shall mean the period between June twenty-fifth, nineteen hundred and fifty and January thirty-first, nineteen hundred and fifty-five, both dates inclusive.

“Vietnam veteran” shall mean (1) any person who performed such wartime service during the period commencing August fifth, nineteen hundred and sixty-four and ending on May seventh, nineteen hundred and seventyfive, both dates inclusive, or (2) any person who served at least one hundred and eighty days of active service in the armed forces of the United States during the period between February first, nineteen hundred and fifty-five and August fourth, nineteen hundred and sixty-four; provided, however, that for the purposes of the application of the provisions of chapter thirty-one, it shall also include all active service between the dates May seventh, nineteen hundred and seventy-five and June fourth, nineteen hundred and seventy-six; and provided, further, that any such person who served in said armed forces during said period and was awarded a service-connected disability or a Purple Heart, or who died in said service under conditions other than dishonorable, shall be deemed to be a veteran notwithstanding his failure to complete one hundred and eighty days of active service.

“Lebanese peace keeping force veteran” shall mean any person who performed such wartime service and received a campaign medal for such service during the period commencing August twenty-fifth, nineteen hundred and eighty-two and ending when the President of the United States shall have withdrawn armed forces from the country of Lebanon.

“Grenada rescue mission veteran” shall mean any person who performed such wartime service and received a campaign medal for such service during the period commencing October twenty-fifth, nineteen hundred and eighty-three to December fifteenth, nineteen hundred and eighty-three, inclusive.

“Panamanian intervention force veteran” shall mean any person who performed such wartime service and received a campaign medal for such service during the period commencing December twentieth, nineteen hundred and eighty-nine and ending January thirty-first, nineteen hundred and ninety.

“Persian Gulf veteran” shall mean any person who performed such wartime service during the period commencing August second, nineteen hundred and ninety and ending on a date to be determined by presidential proclamation or executive order and concurrent resolution of the Congress of the United States. “WAAC” shall mean any woman who was discharged and so served in any corps or unit of the United States established for the purpose of enabling women to serve with, or as auxiliary to, the armed forces of the United States and such woman shall be deemed to be a veteran.

None of the following shall be deemed to be a “veteran”:

(a) Any person who at the time of entering into the armed forces of the United States had declared his intention to become a subject or citizen of the United States and withdrew his intention under the provisions of the act of Congress approved July ninth, nineteen hundred and eighteen.

(b) Any person who was discharged from the said armed forces on his own application or solicitation by reason of his being an enemy alien.
(c) Any person who has been proved guilty of willful desertion.
(d) Any person whose only service in the armed forces of the United States consists of his service as a member of the coast guard auxiliary or as a temporary member of the coast guard reserve, or both.
(e) Any person whose last discharge or release from the armed forces is dishonorable.
"Armed forces" shall include army, navy, marine corps, air force and coast guard.
"Active service in the armed forces", as used in this clause shall not include active duty for training in the army national guard or air national guard or active duty for training as a reservist in the armed forces of the United States.
Forty-fourth, "Registered mail", when used with reference to the sending of notice or of any article having no intrinsic value shall include certified mail.
Forty-fifth, "Pledge", "Mortgage", "Conditional Sale", "Lien", "Assignment" and like terms, when used in referring to a security interest in personal property shall include a corresponding type of security interest under chapter one hundred and six of the General Laws, the Uniform Commercial Code.
Forty-sixth, "Forester", "state forester" and "state fire warden" shall mean the commissioner of environmental management or his designee.
Forty-seventh, "Fire fighter", "fireman" or "permanent member of a fire department", shall include the chief or other uniformed officer performing similar duties, however entitled, and all other fire officers of a fire department, including, without limitation, any permanent crash crewman, crash boatman, fire controlman or assistant fire controlman employed at the General Edward Lawrence Logan International Airport, or members of the Massachusetts military reservation fire department.
Forty-eighth, "Minor" shall mean any person under eighteen years of age.
Forty-ninth, "Full age" shall mean eighteen years of age or older.
Fiftieth, "Adult" shall mean any person who has attained the age of eighteen.
Fifty-first, "Age of majority" shall mean eighteen years of age.
Fifty-second, "Superior court" shall mean the superior court department of the trial court, or a session thereof for holding court.
Fifty-third, "Land court" shall mean the land court department of the trial court, or a session thereof for holding court.
Fifty-fourth, "Probate court", "court of insolvency" or "probate and insolvency court" shall mean a division of the probate and family court department of the trial court, or a session thereof for holding court.
Fifty-fifth, "Housing court" shall mean a division of the housing court department of the trial court, or a session thereof for holding court.
Fifty-sixth, "District court" or "municipal court" shall mean a division of the district court department of the trial court, or a session thereof for holding court, except that when the context means something to the contrary, said words shall include the Boston municipal court department.
Fifty-seventh, "Municipal court of the city of Boston" shall mean the Boston municipal court department of the trial court, or a session thereof for holding court.
Fifty-eighth, "Juvenile court" shall mean a division of the juvenile court department of the trial court, or a session thereof for holding court.
CREDIT(S)
Amended by St.1934, c. 283; St.1935, c. 26; St.1936, c. 180; St.1937, c. 38; St.1938, c. 245; St.1941, c. 91, § 1; St.1941, c. 509, § 1; St.1945, c. 242, § 1; St.1945, c. 637, § 1; St.1946, c. 190; St.1948, c. 241; St.1951, c. 215, § 1; St.1953, c. 319, § 2; St.1954, c. 128, § 1; St.1954, c. 627, § 1; St.1955, c. 99, §§ 1, 2; St.1955, c. 403, § 1; St.1955, c. 683; St. 1956, c. 281, §§ 1, 2; St.1957, c. 164, § 1; St.1957, c. 765, § 3; St.1958, c. 140; St.1958, c. 626, § 1; St.1960, c. 299; St.1960, c. 544, § 1; St.1960, c. 812, § 1; St.1962, c. 427, § 1; St.1962, c. 616, § 1; St.1964, c. 322; St.1965, c. 875, §§ 1, 2; St.1966, c. 716; St.1967, c. 437; St.1967, c. 844, § 23; St.1968, c. 24, § 1; St.1968, c. 531, § 1; St.1969, c. 544, § 1; St.1969, c. 831, § 2; St.1970, c. 215, § 1; St.1973, c. 925, § 1; St.1973, c. 1050, § 1; St.1974, c. 205, § 1; St.1974, c. 493, § 1; St.1975, c. 706, § 2; St.1976, c. 112, § 1; St.1976, c. 156; St.1977, c. 130;

St.1977, c. 691, § 1; St.1977, c. 977; St.1978, c. 12; St.1978, c. 247; St.1978, c. 478, § 2; St.1979, c. 230; St.1982, c. 189, § 2; St.1983, c. 113; St.1984, c. 363, §§ 1 to 4; St.1985, c. 114; St.1985, c. 220; St.1985, c. 451, § 1; St.1986, c. 534, §§ 1, 2; St.1987, c. 465, §§ 1, 1A; St.1987, c. 522, § 1; St.1987, c. 587, § 1; St.1988, c. 180, § 1; St.1989, c. 665, § 1; St.1991, c. 109, §§ 1, 2; St.1992, c. 133, § 169; St.1992, c. 286, § 1; St.1992, c. 403, § 1; St.1996, c. 204, § 3; St.1996, c. 450, §§ 1 to 4; St.2002, c. 313, § 1; St.2004, c. 116, § 1, eff. Aug. 26, 2004; St.2004, c. 122, § 2, eff. Sept. 1, 2004; St.2004, c. 149, § 8, eff. July 1, 2004; St.2004, c. 349, eff. Dec. 15, 2004; St.2005, c. 130, § 1, eff. Nov. 11, 2005; St.2007, c. 109, § 1, eff. Dec. 5, 2007; St.2008, c. 176, § 2, eff. July 8, 2008; St.2008, c. 308, § 1, eff. Sept. 1, 2008; St.2008, c. 445, § 1, eff.

Mar. 30, 2009.
Current through Chapter 10 of the 2009 1st Annual Sess.

END OF DOCUMENT
M.G.L.A. 4 § 7 Page 11

Effective:[See Text Amendments]
Massachusetts General Laws Annotated Currentness
Part I. Administration of the Government (Ch. 1-182)
Title II. Executive and Administrative Officers of the Commonwealth (Ch. 6-28A)
Chapter 6. The Governor, Lieutenant Governor and Council, Certain Officers Under the Governor and Council, and State Library (Refs & Annos)

§ 172. Dissemination of record information; certification; eligibility for access; scope of inquiry; listing; access limited; rules; use of information except as otherwise provided in this section and sections one hundred and seventy-three to one hundred and seventy- five, inclusive, criminal offender record information, and where present, evaluative information, shall be disseminated, whether directly or through any intermediary, only to (a) criminal justice agencies; (b) such other agencies and individuals required to have access to such information by statute including United States Armed Forces recruiting offices for the purpose of determining whether a person enlisting has been convicted of a felony as set forth in Title 10, section 504 of the United States Code; to the active or organized militia of the commonwealth for the purpose of determining whether a person enlisting has been convicted of a felony, and (c) any other agencies and individuals where it has been determined that the public interest in disseminating such information to these parties clearly outweighs the interest in security and privacy. The extent of such access shall be limited to that necessary for the actual performance of the criminal justice duties of criminal justice agencies under clause (a); to that necessary for the actual performance of the statutory duties of agencies and individuals granted access under clause (b); and to that necessary for the actual performance of the actions or duties sustaining the public interest as to agencies or individuals granted access under clause (c). Agencies or individuals granted access under clause (c) shall be eligible to receive criminal offender record information obtained through interstate systems if the board determines that such information is necessary for the performance of the actions or duties sustaining the public interest with respect to such agencies or individuals. The board shall certify those agencies and individuals requesting access to criminal offender record information that qualify for such access under clauses (a) or (b) of this section, and shall specify for each such agency or individual certified, the extent of its access. The board shall make a finding in writing of eligibility, or noneligibility of each such agency or individual which requests such access. No such information shall be disseminated to any agency or individual prior to the board's determination of eligibility, or, in cases in which the board's decision is appealed,

prior to the final judgment of a court of competent jurisdiction that such agency or individual is so eligible.

No agency or individual shall have access to criminal offender record information under clause (c), unless the board, by a two-thirds majority of the members present and voting, determines and certifies that the public interest in disseminating such information to such party clearly outweighs the interest in security and privacy. The extent of access to such information under clause (c) shall also be determined by such a two-thirds majority vote of the board. Certification for access under clause (c) may be either access to information relating to a specific identifiable individual, or individuals, on a single occasion; or a general grant of access for a specified period of time not to exceed two years. A general grant of access need not relate to a request for access by the party or parties to be certified. Except as otherwise provided in this paragraph the procedure and requirements for certifying agencies and individuals under clause (c) shall be according to the provisions of the preceding paragraphs of this section.

Each agency holding or receiving criminal offender record information shall maintain, for such period as the board shall determine, a listing of the agencies or individuals to which it has released or communicated such information.

Such listings, or reasonable samples thereof, may from time to time, be reviewed by the board or the council to determine whether any statutory provisions or regulations have been violated.

Dissemination of criminal offender record information shall, except as provided in this section and for purposes of research programs approved under section one hundred and seventy-four, be permitted only if the inquiry is based upon name, fingerprints, or other personal identifying characteristics. The board shall adopt rules to prevent dissemination of such information where inquiries are based upon categories of offense or data elements other than said characteristics; provided, however, that access by criminal justice agencies to criminal offender record information on the basis of data elements other than personal identifying characteristics, including but not limited to, categories of offense, mode of operation, photographs and physical descriptive data generally, shall be permissible, except as may be limited by the regulations of the board. Except as authorized by this chapter it shall be unlawful to request or require a person to provide a copy of his criminal offender record information. At the time of making any criminal record inquiry pursuant to clause (b) or (c) of the first paragraph of this section, the party certified to receive criminal offender record information shall submit to the board an acknowledgement that such inquiry will be undertaken, signed by the person who is the subject of such inquiry on a form prepared or approved by the board.

Notwithstanding any other provisions of this section, the following information shall be available to any person upon request: (a) criminal offender record information consisting of conviction data; provided, however, that all requests for such conviction data shall be made to the board; and provided, further, that the board shall disclose only conviction data which it maintains in a standardized format in its automated criminal history file, and (b) information indicating custody status and placement within the correction system; provided, however, that no information shall be disclosed that identifies family members, friends, medical or psychological history, or any other personal information unless such information is directly relevant to such release or custody placement decision, and no information shall be provided if its release would violate any other provisions of state or federal law. The parole board, except as required by section one hundred and thirty of chapter one hundred and twentyseven, the department of correction, a county correctional authority, or a probation department with the approval of a justice to the appropriate division of the trial court, may, in its discretion, make available a summary, which may include references to evaluative information, concerning a decision to release an individual on a permanent or temporary basis, to deny such release, or to change his custody status. Information shall be provided or made available pursuant to the preceding paragraph only if the individual named in the request or summary has been convicted of a crime punishable by imprisonment for a term of five years or more, or has been convicted of any crime and sentenced to any term of imprisonment, and at the time of the request: is serving a sentence of probation or incarceration, or is under the custody of the parole board; or having been convicted of a misdemeanor, has been released from all custody or supervision for not more than one year; or having been convicted of a felony, has

been released from all custody or supervision for not more than two years; or, having been sentenced to the custody of the department of correction, has finally been discharged therefrom, either having been denied release on parole or having been returned to penal custody for violation of parole, for not more than three years. In addition to the provisions of the preceding sentence, court records for all criminal cases shall be made available for public inspection for a period of one week following conviction and imposition of sentence.

Any individual or agency, public or private, that receives or obtains criminal offender record information, in violation of the provisions of this statute, whether directly or through any intermediary, shall not collect, store, disseminate, or use such criminal offender record information in any manner or for any purpose. Notwithstanding the provisions of this section, the dissemination of information relative to a person's conviction of automobile law violations as defined by section one of chapter ninety C, or information relative to a person's charge of operating a motor vehicle while under the influence of intoxicating liquor which resulted in his assignment to a driver alcohol program as described in section twenty-four D of chapter ninety, shall not be prohibited where such dissemination is made, directly or indirectly, by the motor vehicle insurance merit rating board established pursuant to section one hundred and eighty-three of chapter six, to an insurance company doing motor vehicle insurance business within the commonwealth, or to such insurance company's agents, independent contractors or insurance policyholders to be used exclusively for motor vehicle insurance purposes. Notwithstanding the provisions of this section or chapter sixty-six A, the following shall be public records: (1) police daily logs, arrest registers, or other similar records compiled chronologically, provided that no alphabetical arrestee, suspect, or similar index is available to the public, directly or indirectly; (2) chronologically maintained court records of public judicial proceedings, provided that no alphabetical or similar index of criminal defendants is available to the public, directly or indirectly; (3) published records of public court or administrative proceedings, and of public judicial administrative or legislative proceedings; and (4) decisions of the parole board as provided in section one hundred and thirty of chapter one hundred and twenty-seven.

CREDIT(S)

Added by St.1972, c. 805, § 1. Amended by St.1977, c. 365, § 1; St.1977, c. 691, § 4; St.1977, c. 841; St.1982, c. 31; St.1989, c. 268, § 1; St.1990, c. 177, § 6; St.1990, c. 319, §§ 7 to 12.

Current through Chapter 10 of the 2009 1st Annual Sess.

END OF DOCUMENT

M.G.L.A. 6 § 172 Page 3

Effective:[See Text Amendments]

Massachusetts General Laws Annotated Currentness

Part I. Administration of the Government (Ch. 1-182)

Title II. Executive and Administrative Officers of the Commonwealth (Ch. 6-28A)

Chapter 12. Department of the Attorney General, and the District Attorneys (Refs & Annos)

§ 11H. Violations of constitutional rights; civil actions by attorney general; venue

Whenever any person or persons, whether or not acting under color of law, interfere by threats, intimidation or coercion, or attempt to interfere by threats, intimidation or coercion, with the exercise or enjoyment by any other person or persons of rights secured by the constitution or laws of the United States, or of rights secured by the constitution or laws of the commonwealth, the attorney general may bring a civil action for injunctive or other appropriate equitable relief in order to protect the peaceable exercise or enjoyment of the right or rights secured.

Said civil action shall be brought in the name of the commonwealth and shall be instituted either in the superior court for the county in which the conduct complained of occurred or in the superior court for

the county in which the person whose conduct complained of resides or has his principal place of business.

CREDIT(S)
Added by St.1979, c. 801, § 1. Amended by St.1982, c. 634, § 4.
Current through Chapter 10 of the 2009 1st Annual Sess.

END OF DOCUMENT
M.G.L.A. 12 § 11H Page 1

Effective: July 8, 2008
Massachusetts General Laws Annotated Currentness
Part I. Administration of the Government (Ch. 1-182)
Title X. Public Records (Ch. 66-66A)
Chapter 66. Public Records (Refs & Annos)

§ 10. Public inspection and copies of records; presumption; exceptions
(a) Every person having custody of any public record, as defined in clause Twenty-sixth of section seven of chapter four, shall, at reasonable times and without unreasonable delay, permit it, or any segregable portion of a record which is an independent public record, to be inspected and examined by any person, under his supervision, and shall furnish one copy thereof upon payment of a reasonable fee. Every person for whom a search of public records is made shall, at the direction of the person having custody of such records, pay the actual expense of such search. The following fees shall apply to any public record in the custody of the state police, the Massachusetts bay transportation authority police or any municipal police department or fire department: for preparing and mailing a motor vehicle accident report, five dollars for not more than six pages and fifty cents for each additional page; for preparing and mailing a fire insurance report, five dollars for not more than six pages plus fifty cents for each additional page; for preparing and mailing crime, incident or miscellaneous reports, one dollar per page; for furnishing any public record, in hand, to a person requesting such records, fifty cents per page. A page shall be defined as one side of an eight and one-half inch by eleven inch sheet of paper.
(b) A custodian of a public record shall, within ten days following receipt of a request for inspection or copy of a public record, comply with such request. Such request may be delivered in hand to the office of the custodian or mailed via first class mail. If the custodian refuses or fails to comply with such a request, the person making the request may petition the supervisor of records for a determination whether the record requested is public. Upon the determination by the supervisor of records that the record is public, he shall order the custodian of the public record to comply with the person's request. If the custodian refuses or fails to comply with any such order, the supervisor of records may notify the attorney general or the appropriate district attorney thereof who may take whatever measures he deems necessary to insure compliance with the provisions of this section. The administrative remedy provided by this section shall in no way limit the availability of the administrative remedies provided by the commissioner of administration and finance with respect to any officer or employee of any agency, executive office, department or board; nor shall the administrative remedy provided by this section in any way limit the availability of judicial remedies otherwise available to any person requesting a public record.
If a custodian of a public record refuses or fails to comply with the request of any person for inspection or copy of a public record or with an administrative order under this section, the supreme judicial or superior court shall have jurisdiction to order compliance.
(c) In any court proceeding pursuant to paragraph (b) there shall be a presumption that the record sought is public, and the burden shall be upon the custodian to prove with specificity the exemption which applies.

(d) The clerk of every city or town shall post, in a conspicuous place in the city or town hall in the vicinity of the clerk's office, a brief printed statement that any citizen may, at his discretion, obtain copies of certain public records from local officials for a fee as provided for in this chapter.

The executive director of the criminal history systems board, the criminal history systems board and its agents, servants, and attorneys including the keeper of the records of the firearms records bureau of said department, or any licensing authority, as defined by chapter one hundred and forty shall not disclose any records divulging or tending to divulge the names and addresses of persons who own or possess firearms, rifles, shotguns, machine guns and ammunition therefor, as defined in said chapter one hundred and forty and names and addresses of persons licensed to carry and/or possess the same to any person, firm, corporation, entity or agency except criminal justice agencies as defined in chapter six and except to the extent such information relates solely to the person making the request and is necessary to the official interests of the entity making the request.

The home address and home telephone number of law enforcement, judicial, prosecutorial, department of youth services, department of children and families, department of correction and any other public safety and criminal justice system personnel, and of unelected general court personnel, shall not be public records in the custody of the employers of such personnel or the public employee retirement administration commission or any retirement board established under chapter 32 and shall not be disclosed, but such information may be disclosed to an employee organization under chapter 150E, a nonprofit organization for retired public employees under chapter 180 or to a criminal justice agency as defined in section 167 of chapter 6. The name and home address and telephone number of a family member of any such personnel shall not be public records in the custody of the employers of the foregoing persons or the public employee retirement administration commission or any retirement board established under chapter 32 and shall not be disclosed. The home address and telephone number or place of employment or education of victims of adjudicated crimes, of victims of domestic violence and of persons providing or training in family planning services and the name and home address and telephone number, or place of employment or education of a family member of any of the foregoing shall not be public records in the custody of a government agency which maintains records identifying such persons as falling within such categories and shall not be disclosed.

CREDIT(S)

Amended by St.1948, c. 550, § 5; St.1973, c. 1050, § 3; St.1976, c. 438, § 2; St.1978, c. 294; St.1982, c. 189, § 1; St.1982, c. 477; St.1983, c. 15; St.1991, c. 412, § 55; St.1992, c. 286, § 146; St.1996, c. 39, § 1; St.1996, c. 151, § 210; St.1998, c. 238; St.2000, c. 159, § 133; St.2004, c. 149, § 124, eff. July 1, 2004; St.2008, c. 176, § 61, eff. July 8, 2008.

Current through Chapter 10 of the 2009 1st Annual Sess.

END OF DOCUMENT

M.G.L.A. 66 § 10 Page 2

APPENDIX C: INFORMATION DATABASES, SYSTEMS, AND RECORDS*

Tool	Category	BRIC Access
Word processing program	Software	Yes
Spreadsheet program	Software	Yes
Relational database	Software	Yes
Presentation software to include photo manipulation/enhancement	Software	Yes
Internet browser	Software	Yes
Flowcharting software	Software	Yes
Link analysis software	Software	Yes
Database reporting/visualization software	Software	Yes
Mapping software	Software	Yes
Photo enhancement software	Software	Yes
E-mail program to include interoffice with ability to calendar/task	Software	Yes
Desktop search engine for local and network drives	Software	Yes
Telephone analysis software	Software	Yes
Portable Document Format (PDF) creation software	Software	Yes
Virus blockers	Security software	Yes
Internet restriction	Security software	Yes
Firewall	Security software	Yes
Smart Pass or other encryption software	Security software	No
Publication software	Software	Yes
Statistical analysis software	Software	Yes
Data mining/text mining software	Software	Yes
Agency records management system	System and Database Access	Yes
Agency intelligence system	System and Database Access	Yes
Direct unfiltered Internet connection	System and Database Access	Yes
State crime information system	System and Database Access	Yes
National crime information system	System and Database Access	Yes
State driver's license database	System and Database Access	Yes
Commercial databases containing personally identifying information: CLEAR/ACCURINT	System and Database Access	Yes
Regional Information Sharing Systems (RISS)	System and Database Access	Yes
Law Enforcement Online (LEO)	System and Database Access	Yes
Homeland Security Information Network (HSIN)	System and Database Access	Yes
Telephone database	System and Database Access	Yes
Jail management databases	System and Database Access	Yes
Financial Crimes Enforcement Network (FinCEN)	System and Database Access	Yes
Immigration databases	System and Database Access	No
State wage and hour database	System and Database Access	No
State sex offender registries	System and Database Access	Yes
Crime-specific listservs	System and Database Access	Yes
Really Simple Syndication (RSS) readers	System and Database Access	Yes
Intelligence center databases (state, HIDTA, EPIC, NDIC, etc.)	System and Database Access	Yes
State corrections/probation databases	System and Database Access	Yes
Juvenile justice databases	System and Database Access	Yes
Wireless Internet access	System and Database Access	Yes
Cellular telephone and PDA	System and Database Access	Yes

*This list is based on standards outlined in the Department of Justice Global Intelligence Working Group (GIWG) *Analyst Toolbox: A Toolbox for the Intelligence Analyst* guidelines.