# ORDER FORM

## Order Information

| | | | |
|---|---|---|---|
| **Account Name:** | Boston Regional Intelligence Center | **Contract Start Date:** | 2/1/16 |
| **Prepared By:** | Will Catton | **Contract End Date:** | 5/31/16 |
| **Preparation Date:** | 12/10/15 | | |
| | | **Total Amount:** | **$6,700.00** |

## Subscription Term, Billing & Payment Information

| | | | |
|---|---|---|---|
| **Company Name:** | Boston Regional Intelligence Center | **Billing Phone:** | (617) 343-4328 |
| **Billing Name:** | David Carabin | **Billing Fax:** | |
| **Billing Email:** | David.Carabin@pd.boston.gov | | |
| **Billing Address:** | 1 City Hall Plaza, Room 201<br>Boston, MA 02201 | **Payment Method:**<br>**PO Number:** | Invoice<br>[IF APPLICABLE] |
| **Billing Terms:** | Invoices sent ***Annually*** | | |

**Payment Terms:** Due Upon Receipt. Interest accrues at the rate of 1.5% per month 60 days after the invoice date. Invoices 30 days or more past due may result in suspension of Services.

**This Order Form is subject to and governed by the terms and conditions of the Geofeedia Service Agreement posted online at http://www.geofeedia.com/legal/service-agreement/ (unless there is already a Geofeedia Service Agreement in force and effect between you and Geofeedia, in which case the terms of such existing Geofeedia Service Agreement shall govern this Order Form). If for any reason you are unable to view the Geofeedia Service Agreement online at http://www.geofeedia.com/legal/service-agreement, please contact Geofeedia immediately.**

**This Order Form is valid for 60 days from the Preparation Date.**

| | | | |
|---|---|---|---|
| **Customer:** | Boston Regional Intelligence Center | **Geofeedia, Inc.** | |
| Signature: | [signature] | Signature: | |
| Printed: | Ryan Walsh | Printed: | |
| Title: | Deputy Director | Title: | |
| Date: | 12/31/15 | Date: | |



A0001

**Application Services Subscription***
**The Application Services include the following:**

| **Service Edition** | **Total Price** |
|---|---|
| **Standard Service Package**<br>Customer orders the following Standard Package: | $6,700.00 |

**Geofeedia Public Safety Edition**

Total Permitted Users: Thirty (30)

Search
- Real-Time Search Plus
- Keyword Search
- Discovery Search
- Streamer (5)
- Influencer Search

Engage & Share
- Alerts with Boolean Exclusions
- Notification Inbox
- iOS/Android Mobile App

Archive & Analyze
- Unlimited Data
- Unlimited Locations and Recordings
- Analytics
- Translate
- Collections
- CSV Export

Search Radius
- Maximum of 15 kilometers

**Support & Services**
Unlimited Tutorials & Documentation
Customer Support
Customer Success Manager

| | |
|---|---|
| **Total Annual Cost** | **$6,700.00** |

**Order Comments**
For additional details regarding standard features and functionality of the Application Services, please visit:
http://geofeedia.com/how-it-works

January 2020


# 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 9/11 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 that relevant entities, including fusion centers, 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 U.S. 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.

# A. Table of Contents

## A. PURPOSE STATEMENT

The purpose of this privacy, civil rights, and civil liberties protection policy is to help ensure that the Boston Regional Intelligence Center (hereafter "BRIC" or "the center") personnel and individuals assigned to the BRIC comply with applicable federal, state, local, and tribal law and assist 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 public safety matters, including terrorism-related and other criminal activity and information.
- Encouraging individuals or community groups to trust and cooperate with the justice system.
- Promoting governmental legitimacy and accountability.
- Making the most effective use of public resources allocated to public safety agencies.

## B. POLICY APPLICABILITY AND LEGAL COMPLIANCE

1. All BRIC personnel (including, but not limited to, individuals assigned to the BRIC from other agencies and individuals providing various support services) and authorized users will comply with:

   a. Applicable provisions of this privacy policy.

   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 of its personnel 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 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 periodically 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 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. The privacy officer serves as the liaison for the Information Sharing Environment, overseeing implementation of and compliance with the 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 composed of personnel appointed by the bureau chief of the Boston Police Department's Bureau of Intelligence and Analysis. 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
- Is reliable and verifiable or limitations on the quality of the information are identified, and
- Is based on the source agency's good faith belief that 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 (including suspicious activity reports [SARs] and ISE-SARs), subject to BRIC policies, procedures, and guidelines.

2. The BRIC will not seek or retain (and originating agencies will agree not to submit) information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.
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 the 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 e-mail, 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 individuals' 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 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 which 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 for 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 or 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 and leads.
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, via document labeling caveats, 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 §172, M.G.L. c. 12 §11H, M.G.L. c. 41 §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 members 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 and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information the BRIC 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 a 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 an 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 correct, delete, or refrain 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; or,
   b. The center did not have authority to gather the information or to provide the information to another agency.
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 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 with a potential nexus to terrorism.
3. Access to or disclosure of information retained by the BRIC will be provided at designated levels appropriate to the recipient's need and right to know 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. The center will have a mechanism in place 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. In regards to secondary dissemination, 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 §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.G.L. c. 4 §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 §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 nondisclosure, unless otherwise required by law.

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. While most personally identifiable information in records maintained by the BRIC is exempt from disclosure under 2. below, an individual who 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 may obtain a copy of the information and challenge 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 in certain circumstances, including, but not limited to, when:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (M.G.L. c. 4 §7(26)(f)).
   - Disclosure would endanger the health or safety of an individual, an organization, or a 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 §7(26)(a)).
   - Any other production that would violate state and/or federal law, including, but not limited to, M.G.L. c. 4 §7, M.G.L. c. 6 §172, or M.G.L. c. 66 §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 criminal or terrorism-related protected information that (a) is exempt from disclosure, (b) has been or may be shared through the ISE, or (c) is held by the BRIC and 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 or 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.

## 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 ensure that a secure environment exists within the BRIC's facility.
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, as appropriate, to identify the user initiating the query.
7. The BRIC will utilize appropriate mechanisms 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 the 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 law enforcement and homeland security 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 and the National Fusion Center Association Web site (http://new.nfcausa.org/).
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

## 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 (5) 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 or 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. All BRIC personnel will be trained regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy prior to granting access.
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.
    - 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—**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—**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, a computer process, or a 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, a computer process, or a device 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—**Refers to the Boston Regional Intelligence Center (BRIC) and all participating agencies.

**Civil Liberties—**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—**Refers to the government's 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—**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, an agency, or an 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 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 system, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

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

**Identification—**A process whereby a real-world entity is recognized and its identity established. Identity is 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—**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 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 counterterrorism 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 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 SAR Data Repository), 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 SAR Data Repository, 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 that 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.

**Preoperational Planning—**Describes activities associated with a known or particular planned criminal operation or with terrorist operations generally.

**Privacy—**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 IEPDs that contain personal information.

**Privacy Policy—**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—**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—**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 nonprofit 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.
- 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.
- 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.

**Reasonably Indicative—**This operational concept for documenting and sharing suspicious activity reports takes into account the circumstances in which the observation is made, which creates in the mind of the reasonable observer, including a law enforcement officer, an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.

**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 counterterrorism 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—**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.

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

**Source Agency—**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—**The agency or entity providing ISE-SAR information to the SAR Data Repository.

**Suspicious Activity—**Observed behavior reasonably indicative of preoperational planning associated with 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 associated with terrorism or other criminal

activity. SAR information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

**Terrorism Information—**Consistent with Section 1016(a)(4) of 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.

**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 its ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

**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—**The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information in the SAR Data Repository, 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

## What is Geofeedia?

Geofeedia is the only patented*, location-based social media monitoring, analysis and engagement platform for law enforcement. Our solution enables law enforcement agencies to derive social intelligence to understand, in real-time, what's happening at the locations most important to them.

With Geofeedia, you will have the ability to quickly search seven social media sources by geo-location, from a specific address to an entire neighborhood, then filter results by timeframe, keywords or specific individuals.

We have many ways to visualize and analyze social media within our platform. These include: 1) Map View, 2) Collage View, 3) Streamer View, 4) Analytics View, 5) Alerts and notifications, and 6) User Track View.

## Law Enforcement agencies rely on Geofeedia for:

- Targeted surveillance and monitoring
- Tracking users of interest
- Crisis response and management
- Resource allocation
- Live event security efforts
- Source and data evaluation and corroboration
- Community engagement
- Command center operations

*License details, terms and cost included on following pages…*

## What's included in your license?

### Real-time search

- ✓ Search seven social media sources by location and view results in our map or collage views
- ✓ Unlimited data from monitored Geofeeds per this proposal, otherwise limited to the last 24 hours

### Location Monitoring

- ✓ Geofeedia will continuously monitor and record social media from user defined locations providing the ability to perform historical searches and analysis
- ✓ Unlimited number of location recordings and ability to change locations at any time

### Streaming

- ✓ View up to five concurrent live streams of social media per licensed user

### User Track

- ✓ Connect undercover Twitter and Instagram accounts and follow specific users' posts

### Archive and Export

- ✓ Unlimited monitored Geofeeds and archival in secure data warehouse
- ✓ Export Geofeed data to CSV format

### Analytics

- ✓ Filtering by timeframe, keyword and user; trend views by volume, media, keyword and user; detailed view of feed items and associated metadata; curate items in collections

### Alerts

- ✓ Create unlimited email alert notifications triggered by specific keywords, phrases or users
- ✓ Customize Alerts at any time

### Language Translation

- ✓ Translate all content to and from more than 40 different languages

### Hosting and Storage

- ✓ Included

### User Licenses and Data Charges

- ✓ Unlimited number of user licenses (internal BRIC use only)
- ✓ Data includes up to 200,000 items per month
- ✓ Additional data packs available for purchase

*Continued…*

## Support and Training

- ✓ Account set-up, initial location monitoring configuration, ongoing priority support
- ✓ One kick-off training session plus one user-training session per month when requested

**Terms:**

- Initial Term: signed date below to July 31, 2015
- Full payment due upon signing
- List price expires 90 days from date listed above

**Cost Breakdown:**

Option Details: Enterprise license

- Unlimited user licenses (internal BRIC users only)
- Unlimited recorded locations, up to 200,000 posts per month
- Unlimited Alerts
- Setup & training (Waived)

**Total annual investment** **$9,999**

**Signed:** _____ **Printed Name:** David Carabin

**Title:** Director **Date:** 1/13/15

**Billing Contact:** Andrew Murphy **Billing Address:** 1 City Hall Plaza
Room 204
Boston, MA 02201


# Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities

## Guidance and Recommendations

February 2013

A0051

# Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities

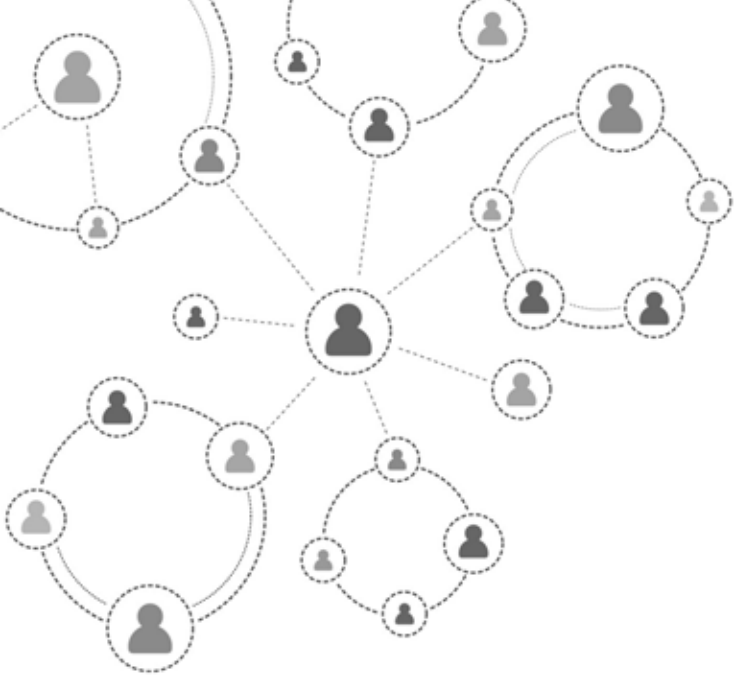
## Guidance and Recommendations

A0053

# Table of Contents



This project was supported by Grant No. 2010-MU-BX-K019 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.



# Executive Summary

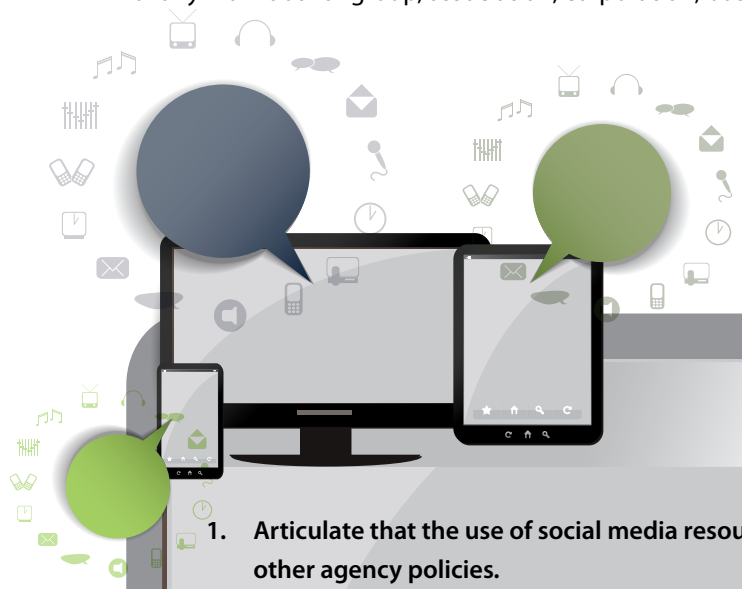
The advent of social media sites has created an environment of greater connection among people, businesses, and organizations, serving as a useful tool to keep in touch and interact with one another. These sites enable increased information sharing at a more rapid pace, building and enhancing relationships and helping friends, coworkers, and families to stay connected. Persons or groups can instantaneously share photos or videos, coordinate events, and/or provide updates that are of interest to their friends, family, or customer base. Social media sites can also serve as a platform to enable persons and groups to express their First Amendment rights, including their political ideals, religious beliefs, or views on government and government agencies. Many government entities, including law enforcement agencies, are also using social media sites as a tool to interact with the public, such as posting information on crime trends, updating citizens on community events, or providing tips on keeping citizens safe.

*Social media sites are increasingly being used to instigate or conduct criminal activity, and law enforcement personnel should understand the concept and function of these sites, as well as know how social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity.*

Social media sites have become useful tools for the public and law enforcement entities, but criminals are also using these sites for wrongful purposes. Social media sites may be used to coordinate a criminal-related flash mob or plan a robbery, or terrorist groups may use social media sites to recruit new members and espouse their criminal intentions. Social media sites are increasingly being used to instigate or conduct criminal activity, and law enforcement personnel should understand the concept and function of these sites, as well as know how social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity. To ensure that information obtained from social media sites for investigative and criminal intelligence-related activity is used lawfully while also ensuring that individuals' and groups' privacy, civil rights, and civil liberties are protected, law enforcement agencies should have a social media policy (or include the use of social media sites in other information-related policies). This social media policy should communicate how information from social media sites can be utilized by law enforcement, as well as the differing levels of engagement—such as apparent/overt, discrete, or covert—with subjects when law enforcement personnel access social media sites, in addition

to specifying the authorization requirements, if any, associated with each level of engagement. These levels of engagement may range from law enforcement personnel "viewing" information that is publicly available on social media sites to the creation of an undercover profile to directly interact with an identified criminal subject online. Articulating the agency's levels of engagement and authorization requirements is critical to agency personnel's understanding of how information from social media sites can be used by law enforcement and is a key aspect of a social media policy.

Social media sites and resources should be viewed as another tool in the law enforcement investigative toolbox and should be used in a manner that adheres to the same principles that govern all law enforcement activity, such as actions must be lawful and personnel must have a defined objective and a valid law enforcement purpose for gathering, maintaining, or sharing personally identifiable information (PII). In addition, any law enforcement action involving undercover activity (including developing an undercover profile on a social media site) should address supervisory approval, required documentation of activity, periodic reviews of activity, and the audit of undercover processes and behavior. Law enforcement agencies should also not collect or maintain the political, religious, or social views, associations, or activities of any individual or group, association, corporation, business, partnership, or organization unless there is a legitimate public safety purpose. These aforementioned principles help define and place limitations on law enforcement actions and ensure that individuals' and groups' privacy, civil rights, and civil liberties are diligently protected. When law enforcement personnel adhere to these principles, they are ensuring that their actions are performed with the highest respect for the



## A Social Media Policy Should Address These Key Elements

1. **Articulate that the use of social media resources will be consistent with applicable laws, regulations, and other agency policies.**
2. **Define if and when the use of social media sites or tools is authorized (as well as use of information on these sites pursuant to the agency's legal authorities and mission requirements).**
3. **Articulate and define the authorization levels needed to use information from social media sites.**
4. **Specify that information obtained from social media resources will undergo evaluation to determine confidence levels (source reliability and content validity).**
5. **Specify the documentation, storage, and retention requirements related to information obtained from social media resources.**
6. **Identify the reasons and purpose, if any, for off-duty personnel to use social media information in connection with their law enforcement responsibilities, as well as how and when personal equipment may be utilized for an authorized law enforcement purpose.**
7. **Identify dissemination procedures for criminal intelligence and investigative products that contain information obtained from social media sites, including appropriate limitations on the dissemination of personally identifiable information.**

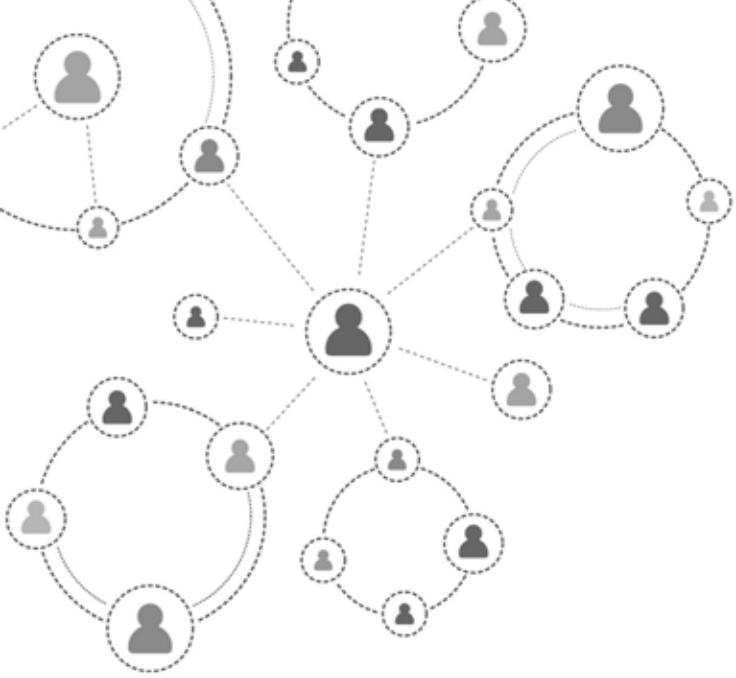
law and the community they serve, consequently fostering the community's trust in and support for law enforcement action.

The Bureau of Justice Assistance (BJA)—with the support of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), a Federal Advisory Committee (FAC) to the U.S. Attorney General on justice-related information sharing, and the Criminal Intelligence Coordinating Council (CICC)—has developed the resource *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations,* which provides law enforcement leadership and policymakers with recommendations and issues to consider when developing policy related to the use of social media information for criminal intelligence and investigative activities. A social media-related policy (or a policy that includes procedures on the use of social media information) will help protect the law enforcement agency and agency personnel and will also help ensure the continued protection of privacy, civil rights, and civil liberties of individuals and groups in the community.

The *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* is designed to guide law enforcement agency personnel through the development of a social media policy by identifying elements that should be considered when drafting a policy, as well as issues to consider when developing a policy, focusing on privacy, civil rights, and civil liberties protections. This resource can also be used to modify and enhance existing policies to include social media information. All law enforcement agencies, regardless of size and jurisdiction, can benefit from the guidance identified in this resource.

The key elements identified in this resource can be applied to "traditional" social media sites (such as Facebook, Twitter, and YouTube) and are also applicable as different and new types of social media sites emerge and proliferate. As a policy is developed, the agency privacy officer and/or legal counsel should be consulted and involved in the process. Additionally, many agencies have an existing privacy policy that includes details on how to safeguard privacy, civil rights, and civil liberties, and an agency's social media-related policy should also communicate how these protections will be upheld when using information obtained from social media sites.

Social media sites have emerged as a method for instantaneous connection among people and groups; information obtained from these sites can also be a valuable resource for law enforcement in the prevention, identification, investigation, and prosecution of crimes. To that end, law enforcement leadership should ensure that their agency has a social media policy that outlines the associated procedures regarding the use of social media-related information in investigative and criminal intelligence activities, while articulating the importance of privacy, civil rights, and civil liberties protections. Moreover, the same procedures and prohibitions placed on law enforcement officers when patrolling the community or conducting an investigation should be in place when agency personnel are accessing, viewing, collecting, using, storing, retaining, and disseminating information obtained from social media sites. As these sites increase in popularity and usefulness, a social media policy is vital to ensuring that information from social media used in criminal intelligence and investigative activities is lawfully used, while also ensuring that individuals' and groups' privacy, civil rights, and civil liberties are diligently protected.



# Introduction

In recent years, social media sites[1] have emerged as a useful tool for friends, coworkers, and families to keep in touch and interact with one another. Persons and groups can share photos or videos, coordinate meet-ups or plans for the weekend, and/or provide updates on newsworthy events to their friends, family, or customer base. One of the goals of these types of sites is instantaneous connections among people, businesses, and organizations, leading to greater and quicker sharing of information and enhanced relationships. Social media sites can also serve as a platform to enable people to express their First Amendment rights, including their political ideals, religious beliefs, or disappointments with government agencies. Many government entities, including law enforcement agencies, are now using social media sites to interact with the public and provide information on crime trends and community events and tips for keeping citizens safe.

*To successfully and lawfully harness the power and value of social media sites, while ensuring that individuals' and groups' privacy, civil rights, and civil liberties are protected, agency leadership should support the development of a policy within their agency regarding the use of social media sites in criminal intelligence and investigative activity.*

In addition to these types of information sharing exchanges between and among persons and entities, social media sites have become a tool that criminals are using for nefarious and criminal purposes. Examples of the use of social media to conduct criminal activity include individuals coordinating a criminal-related flash mob[2] or utilizing a social media site to plan a robbery, online predators joining a social media site to identify and interact with potential victims, and terrorist groups using social media to recruit new members and espouse criminal intentions. Because social media sites are increasingly being used to instigate and conduct criminal activity, law enforcement personnel should understand the concept and function of social media sites and know how social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity.

1 The International Association of Chiefs of Police's (IACP) Center for Social Media defines *social media* as "a category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit)."

2 A *flash mob* is a "group of people, usually organized through social media or text message, that gather at a location to perform a specific action before dispersing. These actions may be for entertainment or criminal purposes." (http://www.IACPsocialmedia.org/glossary)

Social media sites can be valuable sources of information for law enforcement personnel as they fulfill their public safety mission—agency public information officers may use social media to interact with the public, detectives may access social media sites to assist in the identification and apprehension of criminal subjects, intelligence analysts may utilize social media resources as they develop intelligence products regarding emerging criminal activity, and fusion center analysts may use social media resources to assist in the development of analytic assessments. To successfully and lawfully harness the power and value of social media sites, while ensuring that individuals' and groups' privacy, civil rights, and civil liberties are protected, agency leadership should support the development of a policy within their agency regarding the use of social media sites in criminal intelligence and investigative activity.[3]

To assist agencies in drafting a social media policy, the Bureau of Justice Assistance (BJA)—with the support of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), a Federal Advisory Committee (FAC) to the U.S. Attorney General on justice-related information sharing, and the Criminal Intelligence Coordinating Council (CICC)—has developed this resource to provide law enforcement leadership and policymakers with recommendations and issues to consider related to the use of information obtained from social media sites as a part of criminal intelligence and investigative activities.[4]

It is recommended that all law enforcement leadership support the development of a social media-related policy and associated procedures (or enhance existing policies) to guide personnel on accessing, viewing, collecting, storing, retaining, and disseminating (or using) information from social media sites, tools, and resources as a part of their authorized investigative and criminal intelligence activities.[5] A written policy assists in the protection of the agency and agency personnel, as well as the individuals and groups in the community. With the advent of the Internet and, specifically, social media sites, the expectation of privacy has changed. Individuals and groups regularly make openly available various pieces of information of themselves (e.g., photos, relationship links, current locations, dates of birth); while in many cases this information is public and available to anyone with Internet access, law enforcement personnel should use this type of information only based upon a valid law enforcement purpose (i.e., consistent with legal authorities and mission requirements). A policy will assist agency personnel in identifying and understanding their purpose and limitations regarding the use of information from social media sites, the need to document this purpose, and the importance of protecting the public from inadvertent or intentional misuse of information obtained from social media sites.

This resource is designed to identify elements that should be considered for inclusion in a social media policy, issues to consider when developing a policy, and examples of the use of social media as an investigative or intelligence-related tool, focusing on the protection of privacy, civil rights, and civil liberties of individuals and groups. The tenets identified in this resource can be used to draft a new policy or enhance existing information and criminal intelligence-related policies.

3 Agency leadership may also incorporate the tenets identified in the paper into existing policies and procedures (such as policies on criminal intelligence and/or criminal investigations).

4 For purposes of this resource, *law enforcement* may be broadly defined to include all activities related to crime prevention or reduction and the enforcement of the criminal law. However, it is important to note that certain law enforcement or criminal justice agencies may be subject to additional constraints regarding access, use, or disclosure of social media sites and information. For example, prosecutors' offices must adhere to constitutional and statutory discovery and ethical standards that would not apply to police agencies. Consequently, nonpolice law enforcement agencies (such as state attorneys' offices or other prosecutorial entities) will need to take any unique considerations into account in developing a social media policy.

5 For the purpose of this document, accessing, viewing, collecting, storing, retaining, and disseminating information obtained from social media sites, tools, and resources will be referred to as using information obtained from social media sites, tools, and resources.

## Audience


All law enforcement agencies, regardless of size—from a small, rural agency to a large, metropolitan law enforcement agency to a state or urban area fusion center—can benefit from the recommendations identified in this document. As agency policymakers review the components of this resource, it should be understood that social media is, in essence, simply another resource for law enforcement personnel to use in the performance of their public safety mission. The same basic policing principles apply in the use of social media as with other law enforcement action.[6] It is important to provide all agency personnel—from leadership to analysts to detectives and investigators to uniformed patrol officers—with pertinent and applicable guidance to ensure that social media resources are being utilized in a lawful and appropriate manner, a manner that upholds the agency's mission and legal authorities and complies with applicable federal, state, and tribal laws and local ordinances. As agencies develop and adapt a policy on using social media information as a part of their investigative and intelligence-related activities (or enhance existing policies), it is recommended that the agency privacy officer and/or legal counsel be consulted and be involved in the development and implementation process.

## The Protection of Privacy, Civil Rights, and Civil Liberties


As with all law enforcement activity and actions, individuals' privacy, civil rights, and civil liberties must be diligently protected, and the proliferation of social media sites and technology has led to a renewed focus on these protections. Social media resources not only provide a new forum and format for free speech but also introduce a potential risk to individuals' privacy, civil rights, and civil liberties if unauthorized or inappropriate access or use occurs. To mitigate such risks, law enforcement officers and agency personnel are trained to ensure the protection of these rights while performing their duties, be it providing security at a public rally, conducting a criminal investigation, or developing criminal intelligence.[7] This type of training may also be applicable to the use of social media sites in investigative and intelligence activities and the privacy, civil rights, and civil liberties implications associated with access to social media sites and the use of information obtained from such sites.

In addition to training, many agencies have a privacy policy that includes details on how to protect individuals' and groups' privacy, civil rights, and civil liberties.[8] To support and enhance the agency's privacy policy, agencies should also have a policy regarding social media (or enhance existing information and criminal intelligence-related policies) that articulates how these protections will be upheld when using information obtained from social media sites and resources.

6 See the section titled "Law Enforcement Principles" for additional information on these principles.
7 An example of privacy training for line officers is available at http://www.ncirc.gov/training_privacylineofficer.cfm.
8 Additional information on how to develop a privacy policy is available at http://www.it.ojp.gov/privacy.

# Uses of Social Media

Social media may be used by law enforcement personnel in their daily functions in a number of areas, including:

- Pre-employment background investigations
- Outreach and community engagement
- Emergency alerts and notifications
- Analytic assessments
- Situational awareness reports
- Intelligence development
- Criminal investigations

Additional guidance for law enforcement agencies and personnel regarding pre-employment background investigations, outreach and community engagement, and emergency alerts and notifications is accessible via the International Association of Chiefs of Police's (IACP) Center for Social Media Web site, http://www.IACPsocialmedia.org/.

Analytic assessments and situational awareness reports can be designed to provide information to law enforcement on a specific topic to assist agencies in maintaining public safety. These assessments may serve as a gauge for determining the types of criminal activity within a region or determining whether there are threats related to an upcoming public event.[9] Information from social media sites may be referenced in an analytic assessment that identifies current levels of criminal activity within an agency's jurisdiction. For example, an agency may search Twitter feeds, which may contain information on gang-related activities, and Flickr, which may include pictures of gang-related graffiti. This information may then be referenced in an assessment to provide examples of the types of gang activity occurring within a certain area.

As it relates to criminal intelligence development and criminal investigations, information from social media sites may be used as a part of criminal-related background investigative activities. For example, a criminal subject's Facebook page may be accessed to further support the identification of the subject and/or acquaintances. Social media sites and resources may also be used to determine a timeline of events for a suspect. For example, when a person "checks in" on the Web site FourSquare at a certain date and time, this information may be accessible by Facebook users. The individual may then post a picture of himself at this location, which may also be geotagged[10] via a smartphone and uploaded by the individual to Twitter.

There are an ever-increasing number and variety of social media sites: simple Web sites to post short pieces of information, virtual worlds (e.g., Club Penguin, Second Life, massively multiplayer online role-playing games, or online gambling sites), photo-sharing sites, and online forums and comment areas. Although this document will focus on "traditional" social media sites while acknowledging the continuing emergence and proliferation of different types of social media, it should be understood that the elements set forth in this paper may be applied to all types of social media sites and resources.

9 Additional information on responding to First Amendment-protected events is found in the *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*, available at http://it.ojp.gov/documents/First_Amendment_Guidance.pdf.

10 The terms *geolocation/geotagging*, defined at www.IACPsocialmedia.org/glossary, refer to the incorporation of location data in various media, such as, for instance, a photograph, a video, or an SMS message. This may be used on social media platforms to notify people where a user is at a given time.

# Elements of a Social Media Policy

The purpose of a social media policy is to define and articulate acceptable law enforcement practices related to using information obtained from social media sites. As a part of a social media policy, agency leadership should reference other related policies and/or general orders regarding both criminal intelligence and criminal investigations, including an agency's privacy policy or policy regarding undercover activities. Because social media sites can be used to support these functions, it is important to ensure consistency and continuity between policies or orders.

Key elements of a social media policy include:

1. Articulate that the use of social media resources will be consistent with applicable laws, regulations, and other agency policies.

2. Define if and when the use of social media sites or tools is authorized (as well as use of information on these sites pursuant to the agency's legal authorities and mission requirements).

3. Articulate and define the authorization levels needed to use information from social media sites.

4. Specify that information obtained from social media resources will undergo evaluation to determine confidence levels (source reliability and content validity).

5. Specify the documentation, storage, and retention requirements related to information obtained from social media resources.

6. Identify the reasons and purpose, if any, for off-duty personnel to use social media information in connection with their law enforcement responsibilities, as well as how and when personal equipment may be utilized for an authorized law enforcement purpose.

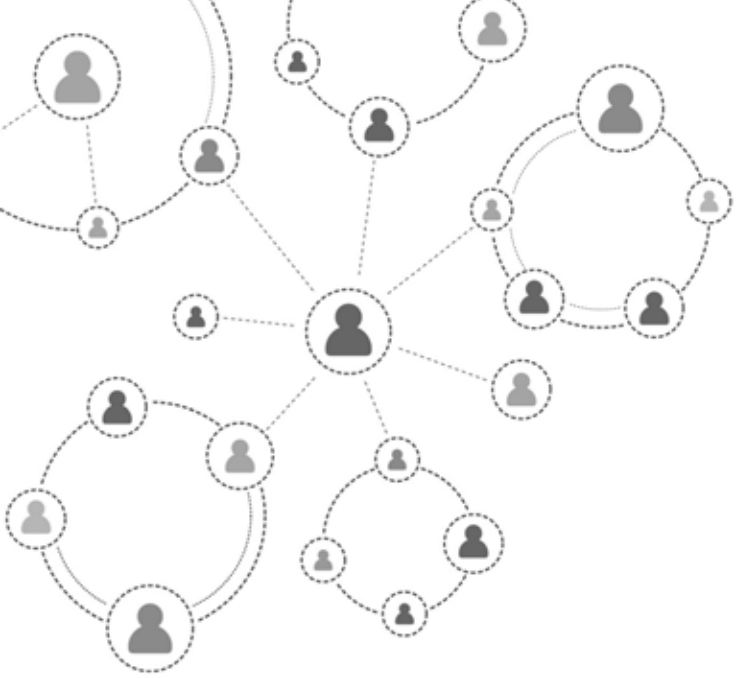
7. Identify dissemination procedures for criminal intelligence and investigative products that contain information obtained from social media sites, including appropriate limitations on the dissemination of personally identifiable information (PII).

# Law Enforcement Principles

Interwoven within these policy elements is the acknowledgement that social media sites and resources are another tool in law enforcement's toolbox of information sources. As such, social media sites and resources should be utilized in a manner that adheres to the same principles that govern all law enforcement actions. These principles include:

- Law enforcement actions must be lawful.
- Law enforcement actions should confirm with community standards, when appropriate.
- Law enforcement actions must have a defined objective and a valid law enforcement purpose for gathering, maintaining, or sharing personally identifiable information about criminal subjects.
- Law enforcement agencies should not collect or maintain information about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless there is a legitimate public safety purpose, such as the information directly relates to criminal conduct or activity. In the case of criminal intelligence, such information should not be collected or maintained unless there is reasonable suspicion to believe that the subject of the information is or may be involved in criminal conduct or activity and the information is directly related to the criminal conduct or activity.
- Law enforcement policy directives must define:
  - » The circumstances under which conduct by personnel is authorized.
  - » The limitations on conduct by personnel.
- All law enforcement officers and support personnel must be properly trained.
- If law enforcement action involves undercover activity, the following areas should be addressed:
  - » Supervisory approval.
  - » Required documentation of activity.
  - » Periodic reviews of activity.
  - » Audit of undercover processes and behavior, including authorization time frames for undercover activities.

Regardless of the tools law enforcement personnel use to perform their duties, these principles help define and place limitations on actions undertaken by personnel and ensure the protection of individuals' and groups' privacy, civil rights, and civil liberties. The implementation of these principles will help ensure that all law enforcement action is performed with the highest respect for the law and for the community and will also help enhance the community's trust in law enforcement.



# Social Media Policy Elements

## Element 1

### Articulate that the use of social media resources will be consistent with applicable laws, regulations, and other agency policies.

**Background:** Social media should be viewed as another tool in the law enforcement toolbox and should be subject to the same policies and guiding principles as other investigative methods and tools, including the identification of reasonable suspicion, a criminal predicate, or a criminal nexus and adherence to the agency's legal authorities and mission requirements.

**Action:** As a part of the agency's authorized law enforcement purpose, social media sites may be accessed to follow up on tips and leads, suspicious activity reports, investigative support, development of criminal intelligence, and the development of situational awareness reports. An agency policy on the use of social media resources as a part of investigative and intelligence-related activities should be similar to agency policies regarding the use of other investigative tools, such as undercover activities or accessing other types of open source information (e.g., Accurint or Internet-based search engines). Further, the social media policy should specify that personnel should be able to articulate the purpose of using information from social media sites, answering the questions "What are you using?" "Why are you using it?" "How did you use it?" and "Is there a time frame on its relevance?"

As a part of this continuity, a social media policy should specifically address:

- When the use of social media sites is authorized.
- The supervisory authorization process (if needed).
- Limitations on using information from social media sites.
- When and how social media sites may be accessed (e.g., during working hours or via agency resources).

## Element 2 Define if and when the use of social media sites or tools is authorized (as well as use of information on these sites pursuant to the agency's legal authorities and mission requirements).

**Background:** Agency leadership and policymakers should be knowledgeable of applicable laws and regulations (including the U.S. Constitution; the Bill of Rights, specifically the Fourth Amendment; the state constitution; other laws; and 28 CFR Part 23) when developing a social media policy and should know how these laws affect using information obtained from social media sites.

Law enforcement has an obligation to comply with the Fourth Amendment. Every person has the right to be free from "unreasonable searches and seizures" of their "persons, houses, papers, and effects." These same protections may also apply towards the use of social media sites—the uploading of pictures, the posting of activities, and the relationships between and among individuals and groups. With the increasing use of technology and the free flow of information on the Internet, it may be difficult to discern what access is reasonable and what would be deemed unreasonable under the Fourth Amendment; therefore, a social media policy should clearly identify reasonable access to social media sites and the use of information obtained from social media sites.

In addition to the Fourth Amendment, the ***Katz*** test[11] establishes a method that can also be utilized as agency personnel analyze public or private information on social media sites. This test, based on ***Katz v. United States***, 389 U.S. 347 (1967), which addresses the expectation of privacy and intent to make information private, could also be applied to the use of social media information, specifically whether a social media site user has exhibited an expectation of privacy in the information and whether the expectation is one that society is ready to recognize as reasonable. For information posted on the Internet (via a social media site) that a user has made no effort to make private or conceal, applying the principles of the *Katz* test would most likely result in a determination that the information is public. However, law enforcement personnel should use that information only when there is an identified, valid law enforcement purpose.

28 CFR Part 23 may also assist agencies as they develop a social media policy. The 28 CFR Part 23 federal regulation has become the de facto national standard regarding criminal intelligence information systems. Although 28 CFR Part 23 regulates systems, many of its tenets may be applicable to a policy regarding social media, such as storage, retention, and sharing of information obtained from social media sites and resources. Additionally, 28 CFR Part 23 states that a project "shall not collect or maintain criminal intelligence information about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity." This overarching purpose statement is also arguably pertinent to information obtained by law enforcement personnel via social media sites, specifically regarding what information personnel can store, retain, and disseminate on political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization.

**Action:** A social media policy should articulate the parameters regarding using information obtained from social media sites. These parameters should be consistent with applicable laws, regulations, and other agency policies and further articulate how privacy, civil rights, and civil liberties protections are upheld during such activities. It is important to note that although information on many social media sites may be "open" (e.g., anyone with Internet access can view the information), ***law enforcement must be mindful of what is legal, as well as what is consistent with community standards and expectations, when using information from a social media site***. In other words, simply because information is

11 See Appendix A for additional information on the ***Katz*** test and decision.

available to law enforcement does not mean it should be used by law enforcement in the absence of a clearly defined and valid law enforcement purpose. For example, a law enforcement investigator should search for and access an individual's Facebook profile when an authorized law enforcement purpose is identified, such as a search for a missing person or further identification of an alleged criminal, and not to look for information on a new neighbor.

Relevant investigative laws, regulations, and policies should also be referenced in a social media policy. Articulating laws, regulations, and policies, as they relate to the use of social media sites and information, will support the agency and personnel in ensuring that they are using social media for a valid law enforcement purpose, adhering to established law enforcement principles, and protecting citizens' and groups' privacy, civil rights, and civil liberties.

Additionally, a social media policy (or policy that addresses information obtained from social media sites) should address the ever-changing nature of social media and associated technology. Technology advancements may affect the access and collection of information from social media sites, and a policy should acknowledge that though technology may change, the foundational elements for accessing social media sites remain consistent, such as accessing social media sites for an authorized law enforcement purpose.

## ELEMENT 3 ARTICULATE AND DEFINE THE AUTHORIZATION LEVELS NEEDED TO USE INFORMATION FROM SOCIAL MEDIA SITES.

**Background:** Social media sites have varying and differing levels of access and engagement, ranging from "following" someone on Twitter to "friending" someone on Facebook or simply searching for an individual or a topic via Google. Engagement levels may also vary, from reviewing publicly available information on a social-networking site to accessing social media resources from a nongovernmental Internet Protocol (IP) address to creating a user profile or account for undercover operations to lawful intercepts of electronic information. Within the different engagement levels are privacy, civil rights, and civil liberties implications. A social media policy should articulate the levels of engagement by law enforcement personnel with subjects when accessing social media sites and also specify the authorization requirements associated with each level.


As part of the levels of engagement, law enforcement personnel should understand privacy settings, end-user licensing agreements, and terms-of-service requirements. Users may regulate their privacy settings on their "profile," which in turn could affect the level-of-engagement parameters. Additionally, companies may articulate law enforcement engagement parameters via a terms-of-service agreement. [12]

12 Many Internet- and communication-based companies have developed guides to assist law enforcement in understanding what information is available and how that information may be obtained. Additional information on these guides is available at the IACP's Center for Social Media, at http://www.IACPsocialmedia.org/investigativeguides.

To assist in understanding how information from social media sites can be used by law enforcement, the graphic above provides a visual demonstration of the comparison between traditional law enforcement practices and specific social media actions. As identified in the graphic, examples of levels of engagement include:

**Apparent/Overt Use—**In the Apparent/Overt Use engagement level, law enforcement's identification need not be concealed. Within this engagement level, there is no interaction between law enforcement personnel and the subject/group. This level of access is similar to an officer on patrol. Information accessed via this level is open to the public (anyone with Internet access can "see" the information). Law enforcement's use and response should be similar to how it uses and responds to information gathered during routine patrol. An example of Apparent/Overt Use would be agency personnel searching Twitter for any indication of a criminal-related flash mob to develop a situational awareness report for the jurisdiction.

Apparent/Overt Use is based on user profiles/user pages being "open"—in other words, anyone with Internet capabilities can access and view the user's information. For instance, if an officer searches for a criminal subject's Facebook page and determines that a profile which appears to be that of the subject has the account privacy settings set to "public" (meaning the information can be viewed by everyone), then the use of that information would be considered Apparent/Overt Use.

The authorization level for Apparent/Overt Use may be minimal, as this level of engagement is considered part of normal, authorized law enforcement activity (based on the law enforcement purpose).

**Discrete Use—**During the Discrete Use engagement level, law enforcement's identity is not overtly apparent. There is no direct interaction with subjects or groups; rather, activity at this level is focused on information and criminal intelligence gathering. The activities undertaken during the Discrete Use phase can be compared to the activities and purpose of an unmarked patrol car or a plainclothes police officer. An example of Discrete Use is an analyst utilizing a nongovernmental IP address to read a Weblog (or blog)[13] written by a known violent extremist who regularly makes threats against the government. Bloggers (those who write or oversee the writing of blogs) may use an analytical tool to track both "hits" to the blog and IP addresses of computers that access the blog, which could potentially identify law enforcement personnel to the blogger. This identification could negatively impact the use of the information and the safety of law enforcement personnel, who would not want to reveal that they are accessing the blog for authorized law enforcement purposes. In many cases, direct supervisory approval may not be necessary within this level of engagement, but the policy should address agency protocol.

**Covert Use—**During the Covert Use engagement level, law enforcement's identity is explicitly concealed. Law enforcement is engaging in authorized undercover activities for an articulated investigative purpose, and the concealment of the officer's identity is essential. An example of Covert Use is the creation of an undercover profile to directly interact with an identified criminal subject online. Another example is an agency lawfully intercepting infomation from a social media site, through a court order, as a part of authorized law enforcement action. Clear procedures should be identified and documented on the use of social media in this phase, since there are many privacy, civil rights, and civil liberties implications associated with Covert Use. Agencies should also review social media sites' information for law enforcement authorities and terms of service for additional information on undercover profiles.

Authorization levels for Covert Use activities should be clearly identified and could be compared to authorization levels needed for any undercover investigative activity (such as undercover narcotics investigations).

**Action:** An agency's social media policy should identify the agency's defined levels of engagement that will be utilized by agency personnel, the types of activity associated with these levels, and direct authorization requirements, if any,

13 For additional information on blogs, please visit http://www.IACPsocialmedia.org/blogfactsheet.

associated with each level from use as a part of official law enforcement activities (e.g., the checking of social media sites is built into the analytic product development process) or direct supervisor approval requirements (such as development of an undercover profile to interact with a criminal subject). For example, if an agency uses social media to gather or disseminate information regarding a First Amendment-related event that has become violent in other jurisdictions, it is essential to clearly define any limits on the collection and use of information from social media.[14]

## Element 4 Specify that information obtained from social media resources will undergo evaluation to determine confidence levels (source reliability and content validity).

**Background:** The evaluation of information—be it for criminal intelligence purposes or for criminal investigative purposes—may have differences. With regard to criminal intelligence, information should be assessed to determine its validity and reliability, and products produced as a result of this information should include proper caveats. In some instances, it may be difficult to determine the validity of information obtained from a social media site (e.g., a citizen submits a tip about a video posted on YouTube depicting a robbery); however, that information may still be considered a potentially valid tip and should be documented as such.

In the case of a criminal investigation, information obtained from a social media site should be further evaluated to ensure that the information is authentic. For example, a video posted on YouTube shows individuals allegedly robbing a convenience store; law enforcement personnel should obtain a subpoena to determine what IP address was used to upload the video and identify to whom the IP address is registered. Information obtained from social media sites can be a valuable tool; however, comprehensive evaluation and authentication are crucial to ensure the reliability and validity of the information and ensure proper caveats are included, as necessary.

Case law has recently been established regarding authentication of information obtained by law enforcement. In ***Griffin v. Maryland***, 2011 Md. LEXIS 226 (Md. 2011), the appeals court ruled that MySpace pages were erroneously admitted into evidence because they had not been properly authenticated. The trial court admitted the postings based on a police officer's testimony that the picture in the profile was of the purported owner and that they had the same location and date of birth. The picture, location, and birth date did not constitute sufficient "distinctive characteristics" to properly authenticate the MySpace printouts of the profile and posting because of the possibility that someone else could have made the profile or had access to it to make the posting. The court stated that there are different concerns when authenticating printouts from social media sites that go beyond the authentication concerns of e-mails, Internet chats, and text messages. Some suggested approaches to the social media authentication issue include an admission by the purported profile owner that it is his or her profile and he or she made the postings in question, a search of the person's computer and Internet history that links the subject to the profile or post, or information obtained directly from the social media site that identifies the person as the profile's owner and the individual with control over it, possibly including IP address identification information. This case demonstrates the need to validate information obtained from social media sites. ***As a source of information for lead development and follow-up, social media can be a valuable tool, but law enforcement personnel should always authenticate and validate any information captured from a social media Web site***.

**Action:** A social media policy should articulate that any information obtained from social media sites be evaluated to determine accuracy, validity, and/or authenticity. Social media interaction and usage are based on user uploads and updates and therefore should not serve as a primary/sole source for information gathering and verification. As with all sources of information, independent validation is important to determine accuracy and, more important, to protect individuals

14 See *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* for additional information on law enforcement's role regarding First Amendment-protected events.

from being incorrectly identified, possibly leading to privacy violations and/or other inappropriate actions. Agencies may also refer to other policies and procedures related to criminal intelligence and investigative activities (and sources of information) as a part of the evaluation and authentication processes of information obtained from social media sites.

## Element 5 Specify the documentation, storage, and retention requirements related to information obtained from social media resources.

**Background:** Based on the purpose for gathering information via social media resources (e.g., intelligence development, analysis assessment, or criminal investigations), agencies should identify the storage and retention requirements (why and for how long this type of information should be retained).[15] For criminal intelligence development and products, agencies may reference the storage and retention requirements identified in 28 CFR Part 23. For the documentation, storage, and retention requirements of information obtained from social media sites that is being utilized for a criminal investigation, agencies should refer to their investigative policies and procedures (and applicable laws and regulations).

If personally identifiable information (PII) (such as a name, a date of birth, or a picture) is identified and collected from social media sites, agencies should be sensitive to the documentation and retention of this information. If the information is part of criminal intelligence development, it is recommended that the tenets of 28 CFR Part 23 be followed; if the information is part of a criminal investigation, it is recommended that agency policy and procedures related to the dissemination of investigative information be referenced.

The documentation of this type of information should specify the purpose of the information use (regardless of the source of information), what information was collected (photos, status updates, friends), when the information was accessed and/or collected, where the information was accessed (identify the Web site), and how the information was collected (open search, nongovernmental IP address, undercover identity, etc.). Copies of the information obtained from the sites should also be documented. Additionally, as law enforcement personnel access social media sites, the reason for the use of the information obtained and the site utilized should be specified in the case or intelligence file.

For analysis assessments, the storage and retention period will be contingent on the assessment findings and whether a valid law enforcement purpose was identified. For example, a local law enforcement agency sends a request for information to the state fusion center to determine whether there are any threats or potential criminal activity associated with an upcoming demonstration. The fusion center creates an awareness assessment and references information obtained from social media resources that articulates that there are no threats identified. Further, the demonstration was peaceful, with no arrests. No potential criminal predicate or criminal nexus was identified either in the assessment itself or during the event, and therefore there is no articulable reason to store the information that was obtained as part of the analysis assessment.

For intelligence development purposes, the requirements of 28 CFR Part 23 should be followed regarding storage and retention of all information, whether collected from social media sites or other information sources. Though not all intelligence systems are required to adhere to 28 CFR Part 23, it has become a de facto national standard,[16] and as such, agencies are strongly encouraged to incorporate the tenets of this regulation into their policies and procedures regarding all criminal intelligence-related information.

15 For additional information on file guidelines for criminal intelligence, please refer to the LEIU *Criminal Intelligence File Guidelines*, http://it.ojp.gov/documents/ncisp/criminal_intel_file_guidelines.pdf.

16 See the *National Criminal Intelligence Sharing Plan*, Recommendation 9, http://it.ojp.gov/documents/NCISP_Plan.pdf.

If information from a social media site was gathered as part of a criminal investigation—such as a photo, identification of associates, or other PII—law enforcement personnel should adhere to agency policies and procedures regarding the documentation and storage of such information, carefully noting when and where the information was gathered.[17] A policy should also address the need to print or record the information gathered from the site to include in the case file for evidentiary purposes, due to the ease of changing social media information (users deleting information, changing their settings, etc.).

**Action:** The documentation, storage, and retention requirements for information obtained from social media resources should be articulated and defined in a social media policy. This section of the policy should be comparable to other investigative and/or intelligence policies regarding information documentation, storage, and retention.

## Element 6 Identify the reasons and purpose, if any, for off-duty personnel to use social media information in connection with their law enforcement responsibilities, as well as how and when personal equipment may be utilized for an authorized law enforcement purpose.

**Background:** The ease and accessibility of social media resources (including the use of applications [or apps] for smartphones and tablet computers) may affect how law enforcement personnel access social media when off duty,[18] as well as the use of personal equipment and personal accounts for official agency purposes. The information that is collected may result in criminal intelligence or lead to an active investigation; therefore, it is important to include a provision in the social media policy to address using information from social media sites for a law enforcement purpose by off-duty personnel and using nonagency equipment for official law enforcement purposes. With greater access to information through social media sites, it may be easier to identify criminal subjects and/or criminal activity, but it is also imperative to identify approved uses and access to the information.

For example, a law enforcement officer is off duty and is posting an update on his Twitter page. As part of his accessing Twitter on his personal computer, he notices a trending topic for his city about a robbery at a jewelry store. The agency's social media policy might require that the officer report this issue to dispatch and conduct a follow-up field incident report, documenting what he viewed, the site where he viewed the information, when he viewed it, and any action based on the information. In another example, an analyst is viewing her friends' status updates on Google+ and notices one friend expressing outrage at recent government policies (the friend does not make any threats, just articulates dissatisfaction). This posting is part of her friend's First Amendment right to free speech, and therefore no law enforcement documentation or other action should take place.

In another example, an intelligence officer who is focused on gang-related crime uses his personal Twitter account to "follow" a subject-matter expert (SME) in the field of gang identification and trends, as authorized in the agency's policy, which includes the provision for law enforcement officers to access social media sites, via personal accounts, as a part of their authorized law enforcement mission. The officer regularly updates his supervisor and intelligence unit members of trends identified by the SME and how these trends may be carried out in the jurisdiction.

Because of the widespread use of social media, agency policy must articulate when and how it is acceptable for off-duty personnel to use information from social media sites as part of their law enforcement mission. Law enforcement personnel

17 It is important to note that the gathering of information from a social media site may be the result of a court-ordered lawful intercept. As such, there may be specific instructions regarding the gathering and storage of information.

18 The IACP's Center for Social Media identifies five key policy considerations for agency policies regarding the use of social media, including the use of social media for personal use. See http://www.iacpsocialmedia.org/GettingStarted/PolicyDevelopment.aspx.

must adhere to law enforcement principles, whether on duty or at home surfing the Internet for a law enforcement purpose.

**Action:** A policy that addresses social media information should specify whether or not off-duty personnel may, as a part of an authorized law enforcement purpose, access social media sites and the reason(s) (if any) and requirements for access. If authorized, the policy should address the parameters in regards to accessing information that is viewed and gathered by off-duty personnel (for an authorized purpose), restrictions on the use of work equipment and/or personal equipment in an official law enforcement capacity while off-duty, and how to document and report the information that is gathered from the social media site. [19]

The policy should also specify whether or not law enforcement personnel may, when carrying out their authorized law enforcement mission and function, use personal equipment (including personal accounts) to access information via social media sites and the reason(s) and requirements associated with the use of personal equipment for this purpose. If the policy indicates that it is acceptable to use personal equipment for official agency purposes, then the policy should also direct personnel to document how information was obtained, the type of information obtained, the reason the information was obtained, and any follow-up action.

## Element 7 Identify dissemination procedures for criminal intelligence and investigative products that contain information obtained from social media sites, including appropriate limitations on the dissemination of personally identifiable information.

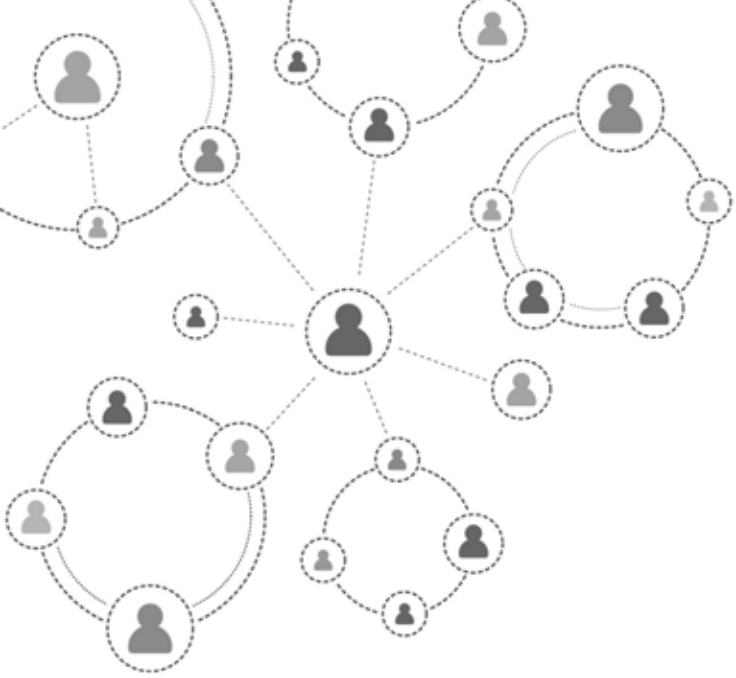
**Background:** Because of the open nature of many types of information obtained from social media sites, it is important to articulate dissemination procedures of products, reports, and requests for information that include information from social media sites.[20]

Additionally, the use of social media sites that focus on advocating greater information sharing among law enforcement agencies and personnel should be addressed in a policy. These sites offer greater access and information sharing capabilities; however, sharing any type of law enforcement information should be limited to nationally recognized sensitive but unclassified (SBU) networks (e.g., Regional Information Sharing Systems® [RISS], Law Enforcement Online [LEO], Homeland Security Information Network [HSIN]) and not social media/open source, commercially developed platforms.

**Action:** A social media policy should address dissemination protocols (who to disseminate to, timeline restrictions, how to disseminate information) for law enforcement reports, products, bulletins, and other types of information that may include information obtained from social media sites (and contain criminal intelligence information, criminal investigative information, and other information containing PII). Additionally, because of the sensitive nature of this type of information, the policy should address the incorporation of a review from a privacy officer and/or general counsel when disseminating products that include information from a social media site (including biographical information, photos, locations of subjects, etc.). A policy should also address dissemination mechanisms, such as using secure e-mail and SBU systems (not open source systems) to share criminal intelligence versus the use of social media sites to post bulletins to educate the public about criminal activity in the community.

19 The IACP's Center for Social Media further addresses employee personal use of social media.

20 For example, the validity and reliability of PII (e.g., photos, videos, and biographical information on a subject) that was obtained from social media sites may be unknown.



# Conclusion

Social media sites and resources may be a helpful tool for law enforcement personnel in the prevention, identification, investigation, and prosecution of crimes. Though social media sites are a relatively new resource for law enforcement, the same principles that govern all law enforcement activities should be adhered to as personnel access, view, collect, use, store, retain, and disseminate information from these types of sites; the same procedures and prohibitions that are placed on law enforcement officers when patrolling the community or conducting an investigation should be in place when law enforcement personnel utilize social media as a part of their public safety function.

*Though social media sites are a relatively new resource for law enforcement, the same principles that govern all law enforcement activities should be adhered to as personnel access, view, collect, use, store, retain, and disseminate information from these types of sites.*

As with other law enforcement tools—such as uniform patrol, undercover activities, and search warrants—it is important to have a policy that articulates the how, when, and why of accessing, viewing, collecting, using, storing, and disseminating information obtained from social media sites, highlighting the privacy, civil rights, and civil liberties protections that are in place, regardless of the information source.

# Appendix A—Cases and Authorities

These cases and authorities were relied on in the construction of the *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* document. While these may be persuasive, it is always prudent to have agency legal counsel examine them in light of the controlling legal authorities in your jurisdiction.

## Fourth Amendment Privacy Law and the Internet

**Expectation of Privacy in Internet Communications**, 92 A.L.R.5th 15, contains a good summary of current law regarding many forms of Internet communication, including e-mail messages and inboxes, chat rooms, Web site content, and social-networking sites. Many cases cited within are summarized below.

***Smith v. Maryland***, 442 U.S. 735 (1979), forms the basis of the "third-party exposure" doctrine of electronic privacy law. In *Smith*, the government used pen register technology to record the numbers dialed out from a certain phone number. This information was used to convict the defendant of robbery. The defendant challenged the use of the pen register as an illegal search under the Fourth Amendment. The court ruled that the defendant did not have a reasonable expectation of privacy in the phone record information because the information was automatically turned over to a third party, the phone company. Even if the defendant had an expectation of privacy in the numbers dialed, it was not one society recognized as reasonable—therefore, there was no Fourth Amendment violation. This case has been analogized to Internet subscriber information, such as account existence and information on who the registered user of the account is because this information is automatically exposed to a third party, the Internet service provider.

***United States v. Jones,*** 132 S. Ct. 945 (2012), is a case involving law enforcement's placement of a Global Positioning System (GPS) device on a subject's car and use of the device to monitor the vehicle's movement on public streets for a four-week period (which extended beyond the period of time and place authorized by a search warrant). The Supreme Court Justices unanimously agreed that use of the GPS device constituted a search within the meaning of the Fourth Amendment. The majority explained that a physical intrusion into a constitutionally protected area, coupled with an attempt to obtain information, can constitute a violation of the Fourth Amendment based upon a theory of common law trespass. The majority explained that "the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Additionally, in a separate opinion, one justice suggested that it may be time to rethink all police use of tracking technology, not just long-term GPS, reasoning that "GPS monitoring generates a precise, comprehensive record of a person's public movement that reflects a wealth of detail about her familial, political, religious, and sexual associations…. The government can store such records and efficiently mine them for years to come." The reasoning expressed by the justices in Jones could have broad implications for law enforcement use of social media in such areas as law enforcement personnel access to information from social media sites and the determination as to whether the social media user has a reasonable expectation of privacy due to privacy controls set up by the user.

***United States v. Kennedy***, 81 F. Supp. 2d 1103 (D. Kan. 2000). Relying on *Smith* (above), the District Court of Kansas ruled that the defendant did not have a reasonable expectation of privacy in information knowingly turned over to his Internet service provider, including Internet subscriber information and information associated with his Internet Protocol (IP) address. Divulgence of this information to law enforcement by Road Runner cable did not violate defendant's Fourth Amendment rights. See also ***United States v. Ohnesorge***, 60 M.J. 946 (N.M. Ct. Crim. App. 2005) (the court did not abuse its discretion in refusing to suppress Internet service provider information, specifically subscription information to a news and file access sharing Web site obtained without a warrant. The defendant did not have a reasonable expectation of privacy in the information; the subscription information was never confidential, and the defendant acknowledged that the information could be shared in the terms of service agreement with the site).

## Social Media and Privacy Law

Nathan Petrashek Comment, "**The Fourth Amendment and the Brave New World of Online Social Networking**," 93 Marq. L. Rev. 1495 (summer 2010). This law review article provides a thorough background on social-networking sites and how the two largest, MySpace and Facebook, operate. A current case law summary is provided as well as an explanation of different privacy doctrines and how they can be applied to the social media setting.

***Katz v. United States***, 389 U.S. 347 (1967), provides the foundation for most federal court privacy rulings and doctrines. *Katz* moved away from previous Supreme Court privacy jurisprudence in holding that the Fourth Amendment protects people and not places, overruling the previous "trespass" doctrine of Fourth Amendment protection. Fourth Amendment considerations no longer require a physical invasion or trespass. In this case, police eavesdropped on private conversations from a public telephone booth, and the court found that even though no physical invasion of the phone booth occurred, this was not necessary to constitute a search for purposes of the Fourth Amendment. Police violated the defendant's Fourth Amendment privacy interests by listening to the content of the conversations without a proper warrant. *Katz* established a two-prong test to determine whether the Fourth Amendment is implicated and a search has occurred. If a person, like Katz, has manifested an intent to make the information private *and* society accepts that expectation of privacy as reasonable, then that privacy expectation cannot be violated without following Fourth Amendment warrant requirements.

***Minnesota v. Olson***, 495 U.S. 91 (1990), further explained the application of *Katz* and the two-prong expectation of privacy test. As an overnight guest, the defendant did have an expectation of privacy in the dwelling, and that expectation is recognized by society as reasonable.

***Courtright v. Madigan***, 2009 U.S. Dist. LEXIS 102544 (S.D. Ill. 2009). The defendant was convicted of three separate offenses of producing, possessing, and receipt of child pornography by a repeat offender. The case initiated through a subpoena served on MySpace.com by the Illinois Attorney General's Office in an effort to learn whether any registered sex offenders were using that site. Upon learning the defendant had a MySpace account, investigators took further steps to discover his IP address and learned that this address had offered pornographic images on the file-sharing site Limewire. These discoveries formed the basis of a warrant that uncovered evidence that was used to convict the defendant. The defendant argued that the initial information gathered from MySpace regarding his account violated his protection against unreasonable searches and seizures under the Fourth Amendment. For other procedural reasons, the defendant's appeal was denied, but the court addressed the search issue and, relying on multiple other courts, held that the defendant had no privacy expectation in Internet subscriber information based on the third-party exposure doctrine. The defendant had no expectation of privacy in the fact that his MySpace account existed, so the request for information on that matter did not violate his Fourth Amendment rights.

***Commonwealth v. Proetto***, 771 A.2d 823 (Pa. Super. Ct. 2001). In *Proetto*, the defendant was brought to the attention of police after a 15-year-old female who had been contacted by the defendant in a public chat room turned over logs of chats that contained explicit information and solicited sexual activity from the underage girl. Police asked the informant to cease communication with the defendant but inform them when he was online again. When police were informed that the defendant was online, they entered the chat room the defendant was in, posing as a 15-year-old girl. The defendant made sexually suggestive comments to the "underage female," which law enforcement officers logged. The defendant challenged use of the chat room logs and e-mail messages under the Fourth Amendment and Pennsylvania Wiretap Act. First, for the communication forwarded to police from the underage informant, the court analogized the e-mail and chat communications to letters and found a limited privacy right. As with letters, the expectation of privacy in the information was reasonable until the intended recipient received the information. After that, because the information could easily be forwarded to others, there remains no reasonable expectation of privacy; therefore, there was no Fourth Amendment violation. For the chats, the defendant did not know exactly whom he was speaking to so he did not have a reasonable expectation of privacy. Communications made directly to the undercover officer survive Fourth Amendment challenges under the same reasoning in that the defendant has only limited privacy interests in e-mail communications. Because the defendant communicated freely with the undercover officer and could not verify the officer's identity, he had no reasonable expectation of privacy in the chat communications. The fact that the officer did not identify himself as law enforcement is of no consequence. The Pennsylvania Wiretap Act was not violated because the informant and the police were both the intended recipients and parties to the communication and recorded the messages concurrently with the communication. For similar case law, see ***United States v. Maxwell***, 45 M.J. 406 (C.A.A.F. 1996) (no expectation of privacy found in e-mail communications in child pornography case); ***United States v. Charbonneau***, 979 F. Supp. 1177 (S.D. Ohio 1997) (explaining chat room and privacy expectations around Internet service providers, finding no reasonable expectation of privacy); and ***Ohio v. Turner***, 156 Ohio App. 3d 177 (Ohio Ct. App. 2004) (no expectation of privacy in chat room conversations with undercover agent posing as underage boy).

***Guest v. Leis***, 255 F.3d 325 (6th Cir. 2001). After receiving a tip regarding online obscenity, police began investigating two electronic bulletin board systems. Police assumed an undercover identity to receive a password to the bulletin board, which enabled them to send e-mails to members, post messages, and share pictures, among other things. After viewing pornographic activity, the police obtained subscriber information from the bulletin boards. Defendants filed a class-

action suit citing violation of their Fourth Amendment rights when the police accessed subscriber information for the bulletin boards, which included the subscribers' name, address, birth date, and password. The court concluded that, like other information provided to a third party, this information was not protected by the Fourth Amendment and there is no reasonable expectation of privacy attached to it.

***J.S. v. Bethlehem Area School District***, 757 A.2d 412 (Pa. Commw. Ct. 2000), involved a student's off-campus Web site postings. A student created a Web site with derogatory comments about a teacher and the school administration. As a result of these postings, the student was expelled. The court found that the school did not violate the student's privacy rights when accessing the materials posted on the Web site. The Web site was not password-protected and was available to anyone that came across it on the Internet. The court reasoned that once material is published on a Web site, it is open to the public. If the creator does not take any steps to protect the Web site content and make it private, no expectation of privacy can be said to exist. See also ***Konop v. Hawaiian Airlines, Inc.***, 236 F.3d 1035 (9th Cir. 2001) (employer did not violate employee's privacy rights by accessing public, unprotected Web site postings. *Konop* held there is no expectation of privacy in information posted to public Web sites).

***United States v. Drew***, 259 F.R.D. 449 (C.D. Cal. 2009). This case involved use of a fake MySpace profile that was created and used in violation of the Web site's terms of service contract agreed to by all users. The Central District of California's court found that in some instances, the violation of a terms of service agreement could constitute a misdemeanor offense under the Computer Fraud and Abuse Act. The court vacated the conviction, however, because the statute did not pass the constitutionality void for vagueness test based on the absence of guidelines in the statutory scheme to guide law enforcement and an actual notice requirement. Although involving civilian use of social media, the reasoning and analysis could be useful to guide law enforcement officers who are using social media and fake profiles in undercover investigations.

## Documenting Social Media During an Investigation

Todd G. Shipley, ***Collecting Legally Defensible Online Evidence: Creating a Standard Framework for Internet Forensic Investigations***. Vere Software Investigative Tools. December 2001. Available at http://veresoftware.com/uploads/CollectingLegallyDefensibleOnlineEvidence.pdf. Last accessed June 9, 2011. This document explains the difference between Internet evidence gathering and traditional computer-based evidence gathering. The collection, preservation, and presentation technique for gathering Internet evidence is explained in the document. References to outside sources and summaries of some documentation techniques are also included.

***Kyllo v. United States***, 533 U.S. 27 (2001), establishes the Supreme Court rule on advanced technology use in searches. In *Kyllo*, the police suspected the defendant of growing marijuana inside his residence. They utilized thermal imaging equipment to "peer through" the walls of the home and determine the defendant was growing marijuana. The court of appeals upheld the search on the basis that the defendant did not make any effort to conceal the heat emanating from his home and therefore did not have a reasonable expectation of privacy under the Fourth Amendment. The Supreme Court reversed, holding that the thermal imaging infiltrated the home and did constitute a search under the Fourth Amendment. The Supreme Court ruled that it was a search in violation of the Fourth Amendment because the thermal imaging gained information, through technology not generally used by the public, that could not have otherwise been gained without physical intrusion of the home, a constitutionally protected area without a warrant.

***Hubbard v. MySpace, Inc.***, 2011 U.S. Dist. LEXIS 58249 (S.D. N.Y. 2011), establishes that social-networking sites, such as MySpace, can provide account user information, IP address information, IP address use date and time logs, *and* contents of the user's private messages and sent-message folders to law enforcement in response to a valid subpoena or warrant under the Electronic Communications Privacy Act.

## Authenticating Social Media Evidence

**Authentication of Electronically Stored Evidence, Including Text Messages and E-Mail**, 34 A.L.R.6th 253. This document outlines the state of case law regarding authentication of various electronic communications, including text messages, e-mails, chat and instant messages, and others. This source provides general background on authentication issues with electronically stored communications; however, the agency or office will need to check the jurisdiction's specific requirements.

***Griffin v. Maryland***, 2011 Md. LEXIS 226 (Md. 2011). In a case involving evidence of witness intimidation obtained from a MySpace profile purported to be that of the defendant's girlfriend, the court relied upon officer testimony. Based on the picture on the profile, the defendant's girlfriend's birthday and profile birthday being the same, and the location listed on the profile, it was determined that this was the profile of the defendant's girlfriend. The trial court authenticated the evidence solely on officer testimony regarding the profile's information and admitted it into evidence. On appeal, the court found error because no extrinsic evidence was used to authenticate the profile or posting. The court reasoned that the picture, location, and birth date alone are not sufficient "distinctive characteristics" to authenticate a MySpace profile printout because someone else could have created the page and made the posting.

***Lorraine v. Markel American Insurance Company***, 241 F.R.D. 534 (D. Md. 2007), outlines the various ways digital and Internet-based evidence can be authenticated in court. The opinion analyzes the applicable federal rules of evidence and how they can be applied to electronically stored evidence. The opinion provides a good guide for law enforcement with respect to the type of information needed for the authentication of Internet-based evidence. Specifically, the opinion explores identifying and authenticating characteristics of e-mail messages, Internet Web site postings, text messages and chat room content, computer-stored and -generated data, and digital photographs. Citations to cases in other jurisdictions explaining electronic evidence authentication are also included.

## Successful Use of Social Media Evidence in Investigations and Trials

***U.S. v. Underwood***, 2010 U.S. Dist. LEXIS 134543 (W.D. Ky. 2010), is a case regarding child pornography and enticing a minor charges. The charges originated from an undercover police investigation conducted online with an officer posing as a 13-year-old boy. The investigation was initiated after an anonymous caller to the police tip line reported a possible pedophile operating on the MySpace social-networking Web site. The police officer then created an undercover profile purporting to be a 13-year-old boy and sent a friend request to the defendant. The defendant engaged the undercover officer in communication on the MySpace and Yahoo! Web sites, with much of the conversation having a sexual nature. Based on this initial investigation, subpoenas were served on the Web sites and various Internet service providers, which resulted in identification of the defendant as the various accounts' holder, the IP addresses associated with those accounts, and his home address. This was used to apply for a search warrant of the defendant's house. Evidence was suppressed because the warrant issued was for evidence of child pornography, while the affidavit accompanying the application referred only to the crime of enticing a minor. In this case, redaction of the warrant and partial suppression were not an adequate remedy; however, probable cause had been established by the social media evidence for a warrant to search for evidence of enticing a minor. If not for the discrepancy in the request to search for evidence and a warrant issued for child pornography crimes and the probable cause listed in the application for enticing a minor, the social media evidence would have provided valid probable cause to issue a warrant. See also ***U.S. v. Lee***, 603 F.3d 904 (11th Cir. 2010) (evidence from a social-networking site was sufficient to uphold convictions of attempted enticement of a minor, attempted production of child pornography, and knowing receipt of child pornography even though communications through the site were with an adult and the children were fictitious. Evidence consisted of multiple online conversations between an undercover postal inspector and the defendant and one recorded phone call); ***U.S. v. Schene***, 543 F.3d 627 (10th Cir. 2008) (social media

investigation evidence and computer account activity used to confirm that the defendant was in fact the person at the IP address who received child pornography).

***In the Interest of F.P.***, 878 A.2d 91 (Pa. Super. Ct. 2005), is a case involving a juvenile delinquency charge resulting from an assault. Evidence used to support a finding of delinquency included instant messages sent from the delinquent juvenile to the victim. The juvenile challenged their admission based on improper authentication because no evidence of their source from the Internet service provider or by a computer forensics expert was provided. The court upheld the finding of delinquency and ruled the authentication was proper based on the circumstantial evidence provided at the adjudication hearing. The basis for authenticating the instant messages rested on the facts that the juvenile identified himself with his first name in the conversations, made accusations in the conversations that were consistent with testimony of other witnesses, and referenced the victim reporting the threats to school officials. Moreover, the character of the messages and conversations was consistent with other testimony regarding the juvenile's feelings and actions towards the victim. These circumstantial facts were sufficient to authenticate the instant messages as coming from the delinquent juvenile.

***A.B. v. Indiana***, 885 N.E. 2d 1223 (Ind. 2008), involves alleged threats made by a student against her principal on the MySpace social-networking site. The opinion does not address authentication issues but does provide an overview on how the MySpace site functions and explains the difference between "public" and "private" profiles, groups, and postings. Authentication issues were resolved by student testimony and permission to access the MySpace postings from their profile, which was "friends" with the appellant student's admitted profile.

***Munoz v. State***, 2009 Tex. App. LEXIS 256 (Tex. App. 2009). The defendant challenged, among other things, a criminal street gang enhancement charge. During the course of an assault trial resulting from a drive-by shooting incident, an investigator with the district attorney's office testified as to how to identify gang members and that based on his investigation, the defendant was a gang member. Several MySpace pictures the investigator used to form his opinion on gang involvement were admitted into evidence. The investigator, who maintained a local gang database and was knowledgeable on local gang activity, provided testimony and evidence from his MySpace investigations of the defendant. This testimony, coupled with testimony from other witnesses and evidence recovered from the defendant's room, formed a legally sufficient basis to convict the defendant on the criminal gang enhancement charge.

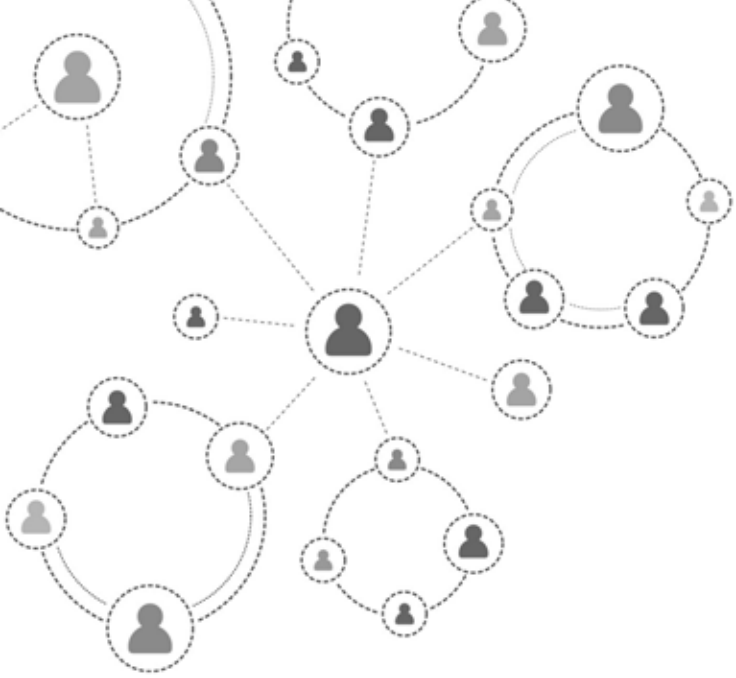
***People v. Chavez***, 2010 Cal. App. Unpub. LEXIS 6186 (Cal. Ct. App. 2010),[21] upheld information charging the defendant's involvement with a criminal street gang. An investigator from the district attorney's office was qualified as a gang expert at trial and testified to common characteristics of gang members and how to identify them. As part of the expert's conclusion that the defendant was an active gang member, the expert relied on a MySpace posting containing a picture of the defendant, the name of the gang, and the defendant's gang moniker. The MySpace evidence and testimony of the expert provided enough of a basis for the information to survive dismissal challenges. See also ***People v. Corleone***, 2009 Cal. App. Unpub. LEXIS 3107 (Cal. Ct. App. 2009)[22] (stalking and criminal threat convictions upheld based on MySpace, e-mail, and text-message evidence); ***People v. Abusharif***, 2011 Ill. App. Unpub. LEXIS 853 (Ill. App. Ct. 2011)[23] (trial court did not abuse discretion in admitting text message and MySpace message evidence in murder trial).

***U.S. v. McNamara-Harvey***, 2010 U.S. Dist. LEXIS 106141 (E. D. Pa. 2010). Anonymous tips that the defendant posted pro-Palestinian/anti-Israeli videos on his Facebook page, as well as personal admissions from the defendant to the Federal Bureau of Investigation (FBI) that he had posted disturbing and/or extremist videos, helped form the basis of a warrant for computer-based evidence of potential terroristic acts.

---

21 This is an unpublished opinion. Please check local court rules when relying on this opinion as authority.
22 See Footnote 21.
23 See Footnote 21.

***Griffin v. Maryland***, 2011 Md. LEXIS 226 (Md. 2011). The appeals court ruled that MySpace pages were erroneously admitted into evidence because they had not been properly authenticated. The trial court admitted the postings based on a police officer's testimony that the picture in the profile was of the purported owner and they had the same location and date of birth. The picture, location, and birth date did not constitute sufficient "distinctive characteristics" to properly authenticate the MySpace printouts of the profile and posting because of the possibility that someone else could have made the profile or had access to it to make the posting. The court stated that there are different concerns when authenticating printouts from social media sites that go beyond the authentication concerns of e-mails, Internet chats, and text messages. Some suggested approaches to the social media authentication issue include an admission of the purported profile owner that it is his or her profile and he/she made the postings in question, a search of the person's computer and Internet history that links the subject to the profile or post, or information obtained directly from the social media site that identifies the person as the profile's owner and individual with control over it, possibly including IP address identification information.



# Appendix B—Georgia Bureau of Investigation Social Media Policy

Georgia Bureau Of Investigation Investigative Division
Directive 8-6-5

Title: Guidelines For The Use Of Social Media By The Investigative Division

Date: October 26, 2012

Reviewed: October 26, 2012

Authority: R. E. Andrews
Deputy Director For Investigations

Page 1 of 12

Purpose: To establish guidelines for the use of social media in pre-employment background investigations, crime analysis and situational assessments, criminal intelligence development, and criminal investigations.

## Definitions

**Crime Analysis and Situational Assessment Reports**—Analytic activities to enable GBI to identify and understand trends, causes, and potential indicia of criminal activity, including terrorism.

**Criminal Intelligence Information**—Data which meets criminal intelligence collection criteria and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals who or organizations which are reasonably suspected of involvement in criminal activity.

**Criminal Nexus**—Established when behavior or circumstances are related to an individual or organization's involvement or planned involvement in criminal activity or enterprise.

**Online Alias**—An online identity encompassing identifiers, such as name and date of birth, differing from the employee's actual identifiers, that uses a nongovernmental Internet Protocol address. Online alias may be used to monitor activity on social media websites or to engage in authorized online undercover activity.

**Online Undercover Activity**—The utilization of an online alias to engage in interactions with a person via social media sites that may or may not be in the public domain (i.e. "friending a person on Facebook").

**Public Domain**—Any Internet resource that is open and available to anyone.

**Social Media**—A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social media networking sites (Facebook, MySpace), micro blogging sites (Twitter), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

**Social Media Monitoring Tool**—A tool used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to make predictive analysis, develop trends, or collect information. Examples include Netbase, Twitterfall, Trackur, Tweetdeck, Socialmention, Socialpointer, and Plancast.

**Social Media Websites**—Sites which focus on building online communities of people who share interests and activities and/or exploring the interests and activities of others. Social media websites are further categorized by Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), micro blogging sites (Twitter, Nixle), photo-and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit). The absence of an explicit reference to a specific social media website does not limit the application of this policy.

**Valid Law Enforcement Purpose**—A purpose for information/intelligence gathering development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, furthering officer safety, and homeland and national security, while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.

## I. GENERAL

Social media may be a valuable investigative tool to detect and prevent criminal activity. Social media has been used for community outreach events such as providing crime prevention tips, providing crime maps, and soliciting tips about unsolved crimes. Social media may also be used to make time sensitive notifications regarding special events, weather emergencies, or missing or endangered persons. While social media is a new resource for law enforcement, employees must adhere to this policy to protect individuals' privacy, civil rights, and civil liberties and to prevent employee misconduct.

## II. UTILIZATION OF SOCIAL MEDIA

**A. Social media may be used by Investigative Division personnel for a valid law enforcement purpose. The following are valid law enforcement purposes:**

1. Pre-employment background investigations;
2. Crime analysis and situational assessment reports;
3. Criminal intelligence development; and
4. Criminal investigations.

**B. While on duty, employees will utilize social media, access social media websites, online aliases, and social media monitoring tools only for a valid law enforcement purpose. The utilization of an online alias or social media monitoring tool for personal use is prohibited and is considered employee misconduct.**

**C. Employees will only utilize social media to seek or retain information that:**

1. Is based upon a criminal predicate or threat to public safety; or
2. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity (criminal intelligence information); or
3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
4. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety; or
5. Is relevant to pre-employment background investigations.

**D. The GBI will not utilize social media to seek or retain information about:**

1. Individuals or organizations solely on the basis of their religious, political, social views or activities; or
2. An individual's participation in a particular non-criminal organization or lawful event; or
3. An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual; or
4. An individual's age other than to determine if someone is a minor.

**E. The GBI will not directly or indirectly receive, seek, accept, or retain information from:**

1. An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if there is reason to believe that the information provider is legally prohibited from obtaining or disclosing the information; or
2. A source that used prohibited means to gather the information.

## III. AUTHORIZATION TO ACCESS SOCIAL MEDIA WEBSITES

This section addresses the authorization necessary to utilize social media and access social media websites for crime analysis and situational awareness/assessment reports; intelligence development; and criminal investigations.

**A. Public Domain**

No authorization is necessary for general research, topical information or other law enforcement uses that do not require the acquisition of an online alias.

**B. Online Alias**

An online alias may only be used to seek or retain information that:

1. Is based upon a criminal predicate or threat to public safety; or

2. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed a criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity; or
3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
4. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety.

**C. Authorization for Online Aliases**

Sworn agents or criminal intelligence analysts must submit a request for an online alias. No other Investigative Division personnel are authorized to submit requests for an online alias or to use an online alias in the performance of their official duties.

The request must contain the following information:

1. Purpose for the request (i.e. type of investigative activity);
2. Username;
3. Identifiers and pedigree to be utilized for the online alias, such as email address, username and date of birth. Do not include password(s) for online aliases and ensure password(s) are secured at all times; and
4. Photograph to be used with online alias, if applicable.

The work unit supervisor must evaluate the request to determine whether an online alias would serve a valid law enforcement purpose. The work unit supervisor must maintain the requests for online alias and their status (approved/denied) for two years from the date of deactivation of the online alias.

Investigative Division personnel with an approved online alias may use their online alias to make false representations in concealment of personal identity in order to establish social media accounts (i.e. a Facebook account). The establishment of a social media account with an approved online alias must be documented.

**D. Authorization for Online Undercover Activity**

1. A sworn agent who has an authorized online alias may also request authorization to engage in online undercover activity. Only agents will be authorized to engage in online undercover activity utilizing the online alias.
2. Online undercover activity occurs when the agent utilizing the online alias interacts with a person via social media. Online undercover operations will only be utilized when there is reason to believe that criminal offenses have been, will be or are being committed (e.g. internet chat rooms where child exploitation occurs).
3. Employees must submit a request to engage in online undercover activity. The request must contain the following information:
    a. Online alias(es) to be used in the online undercover activity;
    b. Social media accounts utilized;
    c. Valid law enforcement purpose; and
    d. Anticipated duration for the online undercover activity.

4. The work unit supervisor must evaluate the request to determine whether online undercover activity is appropriate. If the request is approved, the authorization must be maintained in the file containing the record of the online undercover activity.
5. In situations involving exigent circumstances, the work unit supervisor may provide verbal authorization for online undercover activity. The work unit supervisor should provide written documentation of the request, the exigent circumstances, and the circumstances of the verbal authorization as soon as practical.
6. A record will be maintained of all online undercover activity.
7. Once authorized to engage in online undercover activity, the agent should utilize the appropriate deconfliction system.
8. All approved online undercover activity requests will be reviewed monthly by the work unit supervisor to ensure continued need for the online undercover activity. Approved online undercover activity that does not provide information regarding a valid law enforcement purpose within thirty (30) days will be discontinued.
9. A summary will be placed in the file indicating the date of termination of the online undercover activity. The online alias may be maintained if it is anticipated that it will be utilized again.

## IV. AUTHORIZATION TO UTILIZE SOCIAL MEDIA MONITORING TOOLS

**A. Prior to utilizing a social media monitoring tool, the work unit supervisor will submit a request through the chain of command to the Deputy Director for Investigations for authorization to use the social media monitoring tool. The social media monitoring tool may be utilized in criminal investigations; criminal intelligence development; and crime analysis and situational assessment reports (e.g. during sporting events, demonstrations or other large gatherings that require a law enforcement presence to ensure the safety of the public). The request must contain the following:**

1. A description of the social media monitoring tool;
2. Its purpose and intended use;
3. The social media websites the tool will access;
4. Whether the tool is accessing information in the public domain or information protected by privacy settings; and
5. Whether information will be retained by the GBI and if so, the applicable retention period for such information.

**B. The request must be reviewed by the GBI Privacy Officer prior to approval.**

**C. In exigent circumstances, the work unit supervisor may obtain verbal authorization to utilize the social media monitoring tool and provide written documentation as soon as practical. The written documentation should include a description of the exigent circumstances and the verbal authorization, as well as the required information for the request.**

**D. If approved, the social media monitoring tool may be utilized for a period of ninety (90) days or, in the case of situational assessments such as an event or large gathering, until the conclusion of the law enforcement activity related to the event. After ninety (90) days, the work unit supervisor must submit a summary describing the law enforcement actions that resulted from the use of the social media monitoring tool.**

**If continued use is needed, the summary may also contain a request to continue using the social media monitoring tool. The process to approve the request is the same as the original request.**

## V. SOURCE RELIABILITY AND CONTENT VALIDITY

Information developed from social media sites should be corroborated using traditional investigative tools including interviews, verification of address, verification of internet protocol address information, or other lawful means.

## VI. DOCUMENTATION AND RETENTION

Other than crime analysis and situational assessment reports, all information obtained from social media websites shall be placed within a case file, suspicious activity report, or intelligence report. At no time should Investigative Division personnel maintain any social media files outside of these authorized files.

Crime analysis and situational assessment reports may be prepared for special events management, including First Amendment-protected activities. At the conclusion of the situation requiring the report or First Amendment-protected event where there was no criminal activity related to the information gathered, the information obtained from the social media monitoring tool will be retained for no more than fourteen (14) days. Information from the social media monitoring tool that does indicate a criminal nexus will be retained in an intelligence report, suspicious activity report, or case investigative file as directed by the State of Georgia retention schedule.

Information identified as criminal in nature that is obtained in the course of an investigation from a social media site will be collected and retained using screen shots, printouts of chat logs, copying uniform resource locators (URL's) for subpoena or investigatory purposes, or storing the information via secure digital means. When possible, employees will utilize investigative computer systems and software intended to record data from social media sites.

## VII. OFF DUTY CONDUCT

**A. An employee who becomes aware of potential criminal activity via the Internet while off duty shall contact their supervisor or CEACC if the activity involves a minor child or exigent circumstances to determine the best course of action.**

**B. As soon as practical following awareness of the potential criminal activity, the employee should prepare detailed notes to document a complete description of the information observed and specifics as to the events that occurred or action taken.**

**C. Employees shall act to preserve and maintain proper custody of images, texts, photographs, or other potential evidence.**

## VIII. PERSONAL EQUIPMENT AND PERSONAL SOCIAL MEDIA WEBSITES AND PASSWORDS

Given the ease with which information can be gathered from public internet searches, tracking services, and other computer analytic technology, the use of employee's personal or family internet accounts, social media, or internet service for official GBI business is prohibited.

## IX. DISSEMINATION

Retention and dissemination of social media information will be the same as the type of file, whether a paper or electronic file, in which the information is located. For example, retention and dissemination of social media

information within an intelligence file will be treated in the same manner as an intelligence file. Information developed during the course of a criminal investigation will be located in the investigative case file and retained and disseminated in the same manner as the investigative case file.

## X. EMPLOYMENT BACKGROUND INVESTIGATIONS

As part of its employment background process, Investigative Division personnel will conduct a search of social media websites and profiles in the public domain regarding the applicant. Applicants will be notified that this search will be conducted. Applicants are not required to disclose passwords to social media sites or profiles to the GBI. In the event an applicant discloses their password, the GBI will not utilize the password to log into the applicant's social media site or profile. Employees will not search or attempt to gain access to private social media profiles.

All searches of applicant social media pages and profiles will only search information that is in the public domain.

Online aliases will not be used to conduct employment background investigations.

Only criminal comments or images will be collected as part of the background investigatory process. Employees will not collect or maintain information about the political, religious, or social views, associations or activities of any individual or any group unless such information directly relates to criminal conduct or activity.

During the course of a background investigation, if a reference, supervisor, or colleague of the applicant provides negative information on the applicant related to a social media site, the agent will prepare an investigative summary outlining the information provided by the reference.

## XI. SANCTIONS FOR MISUSE

Any employee who violates the provisions of this directive will be subject to disciplinary action, up to and including termination.

## XII. COMPLAINTS AND INFORMATION QUALITY ASSURANCE

Employees will report violations or suspected violations of this directive to the Privacy Officer in accordance with the GBI Privacy Policy, Directive 7-6 Criminal Intelligence and Privacy Protections, Section VI (D).

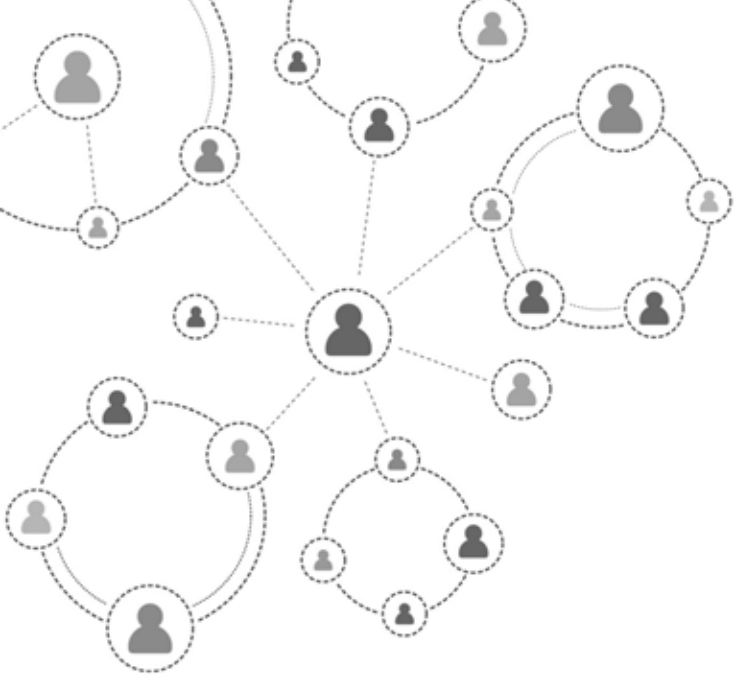
Complaints from the public regarding information obtained from social media websites will be submitted to the Privacy Officer and handled in accordance with the GBI Privacy Policy. If the information is determined to be erroneous, the information will be corrected or deleted.

## XIII. AUDIT

As part of the GBI annual privacy audit, compliance with this directive will be verified by a GBI inspection team led by the Privacy Officer.

## XIV. ANNUAL REVIEW

The GBI Privacy Officer will review this directive at least annually and direct the updating of the policy and procedures as necessary.



# Appendix C—Dunwoody Police Department Social Media Policy

## Dunwoody Police Department Standard Operating Procedure

| | |
|---|---|
| Subject | Social Media |
| Effective Date | November 15, 2011 |
| Sop # | A-50 |
| Reference | Social Media Pages, Blogs, Twitter, Departmental Material, Agency And Personnel Electronic Devices |
| Special Instructions | Annual Review |
| Distribution | All Personnel |
| # Pages | 4 |

## I. PURPOSE

The department endorses the use of social media to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. This policy establishes the department's position on the utility of social media, including management, administration, and oversight. This policy is intended to address social media in general, not a particular form of social media.

## II. POLICY

Social media provides a potentially valuable means of assisting the department and department personnel in meeting community outreach, problem-solving, investigative, crime prevention, and related goals of the department. This policy identifies potential uses that may be explored or expanded upon as directed by the Chief of Police. The personal use of social media can have a bearing on department personnel in their official capacity. As such, this policy provides information of a precautionary nature as well as prohibitions on the use of social media by department personnel.

## III. DEFINITIONS

**Blog**—A self-published commentary on a particular topic that may allow visitors to post responses, reactions, or comments. This term is short for "Web log."

**Page**—The specific portion of a social media website where content is displayed and managed by an individual or individuals.

**Post**—Content an individual shares on a social media site or the act of publishing content on a site.

**Profile**—Information that a user shares about himself or herself on a social networking site.

**Social Media**—A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flicker, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

**Social Networks**—Online platforms where users can create profiles, share information, and socialize with others user a range of techniques.

**Speech**—Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

**Electronic Communications**—Electronic Communications include, among other things, messages, images, data or any other information used in e-mail, instant messages, voice mail, fax machines, computers, personnel digital assistants (including Blackberry or similar text messaging devices), pagers, telephones, cellular and mobile phones including those with cameras, intranet, Internet, back-up storage, information on a memory or flash key or card, jump or zip drive, any other type of internal or external removable storage drives or any other technology tool. In the remainder of this policy, all of these communication devices are collectively referred to as "Systems."

## IV. PROCEDURES

**A. On-the-Job Use / Social Media**

Department-Sanctioned Presence:

1. All department social media sites or pages shall be approved by the Chief of Police in accordance with City of Dunwoody policies.
2. Social media pages shall clearly indicate they are maintained by the department and shall have department contact information displayed.
3. Social media content shall adhere to applicable laws, regulations, and policies, including information technology and records management policies.
4. Content of social media pages is subject to Open Records laws.
5. Department personnel representing the department via social media outlets shall conduct themselves as representatives of the department and the City of Dunwoody and shall adhere to all department and City standards of conduct. They shall identify themselves as members of the department; not make comments regarding the guilt or innocence of suspects or arrestees; not make comments concerning pending prosecutions and not post, transmit or otherwise disseminate confidential information, including pictures, videos, evidence, or other materials in the department relating to training, work assignments, and enforcement efforts without the express written permission of the Chief of Police.
6. Department personnel shall not conduct political activities or private business on departmental social media.
7. The use of departmental computers, telephones, and other electronic communications devices to access social media is prohibited without the authorization of the Chief of Police.

8. Department personnel shall use personal electronic communications devices and computers to manage the department's social media sites only with the express written permission of the Chief of Police.
9. Department personnel shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.

Social media is a valuable tool when seeking evidence or information regarding missing persons, wanted persons, gang activity, crimes perpetrated online, photographs or videos of a crime posted by a participant or observer.

10. Social media can be used for community outreach by providing crime prevention tips, offering online reporting opportunities, sharing crime maps and data, and soliciting tips about unsolved crimes.
11. Social media may be used for time-sensitive notifications of road closures, special events, weather emergencies, and missing or endangered persons.

**B. Personal Use / Social Media**

Precautions and Prohibitions:

1. Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair the work of the department for which confidentiality is important and does not impede the performance of duties.
2. Department personnel are cautioned that representing themselves as employees of the department in their off duty social networking may bring about targeting of the employee. The targeting of law enforcement personnel through social networking sites as a form of retaliation is documented.
3. Department personnel are cautioned that when using social media, their speech becomes part of worldwide electronic domain. Posting of personal photographs and other personal information by departmental personnel may subject them to becoming targets of criminal acts, harassment, or other forms of abuse due to their employment.
4. Department personnel shall adhere to the Code of Conduct when representing themselves as members of the department. They shall not post obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals.
5. Department personnel may not divulge information gained by reason of their authority; make statements, speeches, appearances, and endorsements; or publish materials that could reasonably be considered to represent the views or positions of this department without express authorization of the Chief of Police.

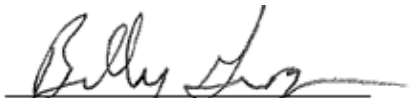
**C. Agency and Personnel Electronic Devices**

Personal Computers, Cell Phones, and Recording Devices:

1. Department personnel and system users may not use personal laptops within any City building or leased space. Additionally, employees and system users may not use personal laptops to gain access to City network resources. Department personnel may have extenuating reasons for using a personal laptop, which must be approved by the Chief of Police.
2. Although incidental and occasional personal use of Systems that does not interfere or conflict with productivity or the City's business or violate City policy is permitted, personal communications in our Systems are treated the same as all other Electronic Communications and will be used, accessed, recorded, monitored, and disclosed by the City at any time without further notice. Since all Electronic Communications and Systems can be accessed without advance notice, employees and system users

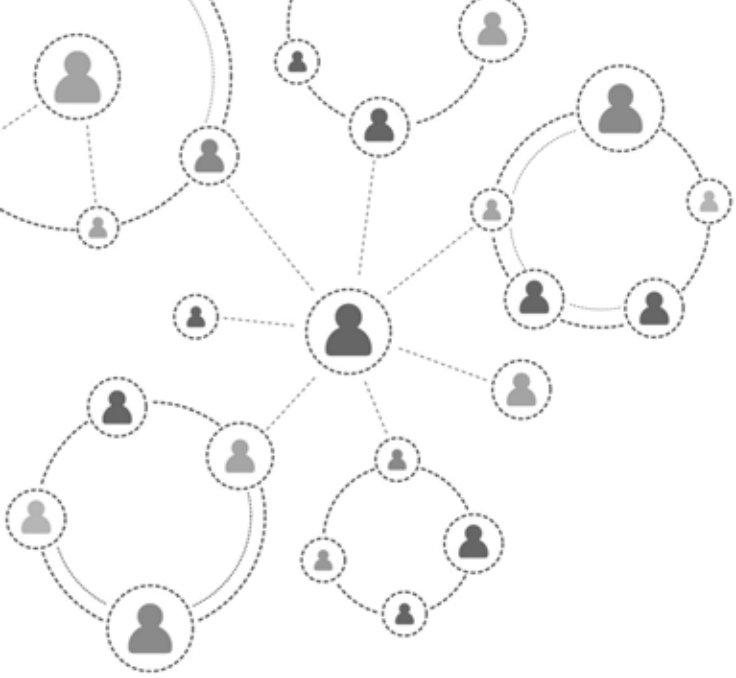
should not use our Systems for communication or information that they would not want revealed to third parties. Employees, therefor, shall not have any expectation of privacy regarding the use of our Systems.

3. The use of personal audio / visual recording devices while on duty and for the performance of assigned duties and responsibilities is prohibited unless otherwise authorized in writing by the Chief of Police.



Billy Grogan, Chief of Police
Dunwoody Police Department

| | |
|---|---|
| First Reading: | 091111 |
| Final Adoption | 101311 |
| Distribution Date | 101411 |
| Effective Date | 111511 |



# Appendix D—New York City Police Department Social Media Policy

Data contained within social network sites may assist law enforcement in gathering timely information in furtherance of crime prevention, preservation of public order, and the investigation of criminal activity, including suspected terrorist activity. These guidelines are promulgated, in part, to instill the proper balance between the investigative potential of social network sites and privacy expectations.

Therefore, effective immediately, when a member of the service requires the use of social network websites to conduct investigations or research, the following procedure will be complied with:

## I. Purpose

To conduct social network-based investigations and research.

## II. Scope

Data contained on the Internet within social network sites may assist law enforcement in gathering timely information in furtherance of crime prevention, including the preservation of public order and the investigation of criminal activity, including suspected terrorist activity. To effectively fulfill these duties, it may be necessary for members of the service to access social network sites using an online alias. No prior authorization is ever required for information contained on publicly available internet sources.

## III. Definitions

**Exigent Circumstances**—For the purpose of this procedure, circumstances requiring action before authorization can be obtained, in order to protect life or substantial property interest; to apprehend or identify a fleeing offender; to prevent the hiding, destruction or alteration of evidence; or to avoid other serious impairment or hindrance of an investigation.

**Online Alias**—An online identity encompassing identifiers, such as name and date of birth, differing from the user's actual name, date of birth, or other identifiers.

**Online Alias Access**—Internet-based searches involving the search and acquisition of information from sites that require an email address, password, or other identifiers for which an online alias is utilized.

**Public Domain Data**—Information accessible through the Internet for which no password, email address, or other identifier is necessary to acquire access to view or collect such information.

**Social Network Site**—Online platform where users can create profiles, share information, or socialize with others using a range of technologies.

| | |
|---|---|
| **Procedure** | **When a member of the service requires access to a social network website for investigative or research purposes:** |
| **Member of the Service** | **1. Confer with supervisor, if access to public domain data requires the use of an online alias/online alias access.**<br>a. No conferral or authorization is required for general research, topical information or other general uses that do not require the acquisition of an online alias/online alias access. |
| | **If application for online alias does not involve suspected terrorist activity:** |
| **Supervisor** | **2. Evaluate request to determine whether an online alias would serve an investigative purpose, and if so, prepare Typed Letterhead requesting an online alias to bureau chief/ deputy commissioner concerned.** |
| | **2. Include on Typed Letterhead:**<br>a. Purpose for the request (i.e., type of investigation, etc.)<br>b. Tax registry number of requesting member<br>c. Username (online alias)<br>d. Identifiers and pedigree to be utilized for the online alias, such as email address, username and date of birth.<br>e. Do not include password(s) for online alias and ensure password(s) are secured at all times.<br>f. Indicate whether there is a need to requisition a Department laptop with aircard. |
| | **4. Review photograph to be used in conjunction with online alias, if applicable.**<br>a. Consider the purpose for which the photograph is being used and the source of the photograph.<br>b. Attach a copy of the approved photograph and indicate on Typed Letterhead how photograph was obtained. |
| | **5. Forward request to commanding officer for review.** |
| **Commanding Officer** | **6. Review request(s) and consider the purpose and whether granting approval would serve an investigative purpose.** |
| | **7. Endorse request(s) indicating APPROVAL/DISAPPROVAL within one day of original request and if APPROVED, immediately forward approval to bureau chief/deputy commissioner concerned, through channels, for informational purposes.** |
| | **8. File copies of requests in command.** |

| | |
|---|---|
| **Member of the Service** | **9. Maintain record of online alias in case records management systems or appropriate Department records.** |
| **Bureau Chief/Deputy Commissioner** | **10. Maintain folder for each APPROVED online alias.**<br>a. Designate an administrator for the online alias. |
| | **If application for online alias involves suspected terrorist activity:** |
| **Supervisor** | **11. Immediately contact Intelligence Division, Operations Desk supervisor and provide details regarding proposed investigation.** |
| **Intelligence Division, Operations Desk Supervisor** | **12. Determine if investigation should be conducted by the Intelligence Division and proceed accordingly.**<br>**13. Notify requesting supervisor to proceed with investigation if it has been determined that the investigation will not be conducted by the Intelligence Division.** |
| **Supervisor** | **14. Comply with steps "2" through "10", as appropriate, if investigation will not be conducted by the Intelligence Division.** |
| | **When exigent circumstances exist that would warrant the immediate use of an online alias:** |
| **Supervisor** | **15. Confer with Intelligence Division, Operations Desk supervisor, if there is concern that the investigation may involve suspected terrorist activity.**<br>a. Comply with instructions from Intelligence Division, Operations Desk supervisor.<br>**16. Confer with commanding officer/executive officer, if investigation does not involve suspected terrorist activity.**<br>**17. Instruct member of the service to proceed with investigation upon receiving APPROVAL from commanding officer/executive officer.**<br>a. Comply with steps "2" through "10", as appropriate, and include in Typed Letterhead, the circumstances that led to the determination of exigent circumstances. |

**Additional Data**

**Legal Considerations**

During the course of an investigation, a member of service may need access to information regarding online accounts maintained by service providers. The federal Electronic Communications Privacy Act (ECPA) governs seizures of electronic evidence. Some information may be obtained with a subpoena; other information requires a special court order; and still other information requires a search warrant. Pertinent sections of the ECPA are as follows:

a. A subpoena is generally deemed sufficient to obtain information such as user information and payment records.

b. Electronic communications, such as email content, in electronic storage for 180 days or less may be obtained only after the issuance of a search warrant, and delayed notification to the subscriber or customer may be ordered if specifically requested in the search warrant application.

c. Electronic communications in electronic storage for more than 180 days may be obtained with a subpoena signed by a judge; however, notice must be provided to the subscriber or customer unless the electronic communications are obtained after the issuance of a search warrant allowing for delayed notification.

**Additional Data (continued)**

d. In anticipation of the issuance of a search warrant, a member of the service may send a request known as a "preservation letter" to an electronic service provider requesting the preservation of electronic records for 90 days, and extend the request for an additional 90 day period.

Note that particular service providers are known to ignore non-disclosure orders (i.e., some service providers will disclose the existence of a search warrant or subpoenas to a subject subscriber or customer.) In general, members of the service should consult with the Legal Bureau before seeking electronic communication through a search warrant or otherwise.

Data obtained through a grand jury subpoena or court order cannot be shared with other law enforcement agencies unless otherwise authorized.

**Operational Considerations**

When a member of the service accesses any social media site using a Department network connection, there is a risk that the Department can be identified as the user of the social media. Given this possibility of identification during an investigation, members of the service should be aware that Department issued laptops with aircards have been configured to avoid detection and are available from the Management Information Systems Division (MISD). A confidential Internet connection (e.g., Department laptop with aircard) will aid in maintaining confidentiality during an investigation. Members who require a laptop with aircard to complete the investigation shall contact MISD Help Desk, upon APPROVAL of investigation, and provide required information.

In addition to using a Department laptop with aircard, members of the service are urged to take the following precautionary measures:

a. Avoid the use of a username or password that can be traced back to the member of the service or the Department;

b. Exercise caution when clicking on links in tweets, posts, and online advertisements;

c. Delete "spam" email without opening the email; and

d. Never open attachments to email unless the sender is known to the member of the service.

Furthermore, recognizing the ease with which information can be gathered from minimal effort from an Internet search, the Department advises members against the use of personal, family, or other non-Department Internet accounts or ISP access for Department business. Such access creates the possibility that the member's identity may be exposed to others through simple search and counter-surveillance techniques.

**Department Policy**

The "Handschu Consent Decree" and "Guidelines for Investigations Involving Political Activity" (see Appendix "A" and "B" of Interim Order 58, series 2004, "Revision to Patrol Guide 212-72, 'Guidelines for Uniformed Members of the Service Conducting Investigations of Unlawful Political Activities'") require that any investigation, including investigations on social networks, by the New York City Police Department involving political activity shall be initiated by and conducted only under the supervision of the Intelligence Division. Accordingly, members of the service shall not conduct investigations on social networks involving political activity without the express written approval of the Deputy Commissioner, Intelligence. Any member of the service who is uncertain whether a particular investigation constitutes an "investigation involving political activity" shall consult with the Legal Bureau.

Members of the service who have created and used online aliases prior to the promulgation of this procedure must submit a request to continue utilizing the alias in accordance with this procedure.

**Related Procedures**

- Citywide Intelligence Reporting System (P.G. 212-12)
- Guidelines for Uniformed Members of the Service Conducting Investigations of Unlawful Political Activities (Interim Order 58, series 2004)

**Forms and Reports** Typed Letterhead

Commanding officers will ensure that the contents of this Order are brought to the attention of members of their commands.

By Direction Of The Police Commissioner

Distribution

All Commands

## About the Global Advisory Committee

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

A0102 Issued 02/13

# ORDER FORM

This order form is subject to and governed by the terms and conditions of Geofeedia's Online Terms of Service posted at http://www.geofeedia.com/terms-of-service. Please review the Online Terms of Service carefully before signing below, as your signature below constitutes your agreement to be bound by its terms. If for any reason you are unable to view the Geofeedia Online Terms of Service online at the website given above, please contact Geofeedia immediately.

Pursuant to this Order Form, Customer is purchasing subscriptions to the Geofeedia Service identified below, subject to any specified usage parameters (e.g. number or types of users, number of locations, volume of data, etc.) and any professional services described herein. The term of this Order Form shall automatically renew for subsequent one-year terms unless either party provides notice to the other party at least forty-five days prior to the Contract End Date.

## Order Information

| | | | |
|---|---|---|---|
| **Account Name:** | Bston Regional Intelligence Center | **Contract Start Date:** | 8/1/2015 |
| **Prepared By:** | Trent McMahan | **Contract End Date:** | 1/31/2016 |
| | | **Total Amount:** | **[$9,999.00]** |

## Subscription Term, Billing & Payment Information

| | | | |
|---|---|---|---|
| **Company Name:** | Boston Regional Intelligence Center | **Billing Phone:** | 617-343-4328 |
| **Billing Name:** | David Carabin | **Billing Fax:** | |
| **Billing Email:** | David.carabin@pd.boston.gov | | |
| **Billing Address:** | 1 City Hall Plaza, Room 201<br>Boston, MA 02201<br>United States | **Payment Method:**<br>**PO Number:** | Invoice<br>[IF APPLICABLE] |
| **Billing Terms:** | Invoices sent ***Annually*** **Customer Initials** DC<br>Invoices for Overage Fees, if any, sent monthly. | | |
| **Payment Terms:** | Due Upon Receipt. Interest accrues at the rate of 1.5% per month 90 days after the invoice date. Invoices 30 days or more past due may result in suspension of Services. | | |

| **Customer: [CUSTOMER NAME]** | **Geofeedia, Inc.** |
|---|---|
| Signature: _____ | Signature: _____ |
| Printed: David Carabin | Printed: _____ |
| Title: Director | Title: _____ |
| Date: June 5, 2015 | Date: _____ |





A0103

**Application Services Subscription***
**The Application Services include the following:**

| **Service Edition** | **Total Price** |
|---|---|

**Standard Service Package**
Customer orders the following Standard Service Package:

**Geofeedia Team Edition** $ 9,999.00

Total Permitted Users: Thirty (30)

Standard Applications
- Real-Time Search
- Up to five (5) Real-Time Streams
- Administrator functions

Premium Applications
- Geofeed Manager (up to 15)
- Collections
- Alerts
- Influencers

Other Included Features
- Shape File Support
- Language Translations
- Data Export
- Analytics
- Networks currently Included: Instagram, Twitter, Flickr, Picasa, YouTube, Facebook, YikYak

Data Storage**
- Up to 200,000 post per month

Search Radius
- Maximum of 15 kilometers

**Additional options** N/A

None

**Training and Implementation** No charge

Geofeedia Video Training (included)

**Total Annual Cost** **$ 9,999.00**

**Order Comments**

* Assuming no Overage Fees.
** Data overage will be billed at a cost of $50.00 per 1,000 posts in excess of per-month allowance.
Note: Any other services not included hereunder and must be identified in a separate, executed Statement of Work.

For additional details regarding standard features and functionality of the Application Services, please visit:
http://geofeedia.com/how-it-works

# OEM Equipment and Supply Pre-Requisition Form

## Requestor Information

| | | | |
|---|---|---|---|
| **Name** | David Carabin | **Discipline** | 508 Law Enforcement |
| **Phone** | 617-343-2748 | ***If other, please indicate*** | |
| **Email (below)** | | **Department/City/Town Name** | 211100 Boston Police |
| david.carabin@pd.boston.gov | | ***If other, please indicate*** | |

[

| Item Description | AEL # (required) | Quantity | Unit Price | Extended Price |
|---|---|---|---|---|
| Geofeedia Social Media Situational Awareness Service | N/A | 1 | $ 9,999.00 | $ 9,999.00 |
| | | 1 | | $ - |
| | | 1 | | $ - |
| | | | | $ - |
| | | | | $ - |
| | | | | $ - |
| **Total** | | | | $ 9,999.00 |

## Specifications

| | | | | | |
|---|---|---|---|---|---|
| **Manufacturer** | | **Make** | | **Model #** | |
| **Part #** | | **Style** | | **Color** | |
| **Size** | | **Useful life** | | **Licensing Required?** | N |
| **Suggested Vendor** | | Geofeedia | | | |
| **Other Information** | | | | | |

## Ship To

| | | | |
|---|---|---|---|
| **Name** | See above | **Department/City/Town Name** | 211100 Boston Police |
| **Phone** | | ***If other, please indicate*** | |
| **Street** | 1 Schroeder Plaza | **City/State/Zip** | Roxbury, MA |

## Jurisdiction Pont of Contact Signature & Date

**Signature** _____ **Date** _____

## City of Boston Use Only

**Request:** Appr / Rej: _____ **Date:** _____

### Header Defaults/PO Comments

| | | | | | |
|---|---|---|---|---|---|
| **GL Unit** | BOSTN | Account Code | 52907 | **Project/Grant** | UASI 13 (HLS14002) |
| **Fund** | 200 | **Dept ID** | 211100 Boston P | **Program (discipline)** | 508 Law Enforcement |
| **Location** | 4480 | **OEM Planner** | A. Murphy | **Program (equip type)** | F Logistical Support |
| **CFDA #** | 97.067 | **Bud Ref** | 0 | **Class (category)** | 23 Equipment |
| **PJ #** | U13-3.3 | AEL # | N/A | **Class (project)** | 04 Intelligence Capacity |

# City of Boston
# Purchase Order



## City of Boston

Purchasing Department
One City Hall
Room 808
Boston MA 02201
United States

| Dispatched | | |
|---|---|---|
| **Purchase Order** | **Date** | **Revision** |
| BOSTN-0000652357 | 2015-01-13 | |
| **Payment Terms** | **Freight Terms** | |
| 00 | DES PPD | |
| **Buyer** | | |
| Habershaw,Deirdre | | |

**Vendor:** 0000078005
Geofeedia, Inc.
444 N. Wells St. Suite 502
Chicago IL 60654
United States

**Bill To:** Auditing Department
One City Hall
Room M-4
Boston MA 02201
United States

**Ship To:** BPD New Police Headquarters
One Schroeder Plaza
Roxbury MA 02120
United States
**Attention:** See Detail Below

**Tax Exempt?** Y **State Tax Exempt ID:** 04-6001380

| Line-Sch | Item/Description | Quantity | UOM | PO Price | Extended Amt | Due Date |
|---|---|---|---|---|---|---|
| 1 - 1 | Geofeedia location-based social media monitoring, analysis, and engagement platform - Through July 31, 2015 | 1.00 | EA | 9999.00 | 9999.00 | 01/18/2015 |
| | | | | Attention: David Carabin-BRIC | | |
| 52907-200-211100-508F-2304-2014-HLS14002 | | 1.00 | | | | |

U13-3.3 - Jan 13, 2015 through July 31, 2015 - trial period
< REAL-TIME SEARCH
Search seven social media sources by location and view results in our map or collage views, Unlimited data from monitored Geofeeds per this proposal, otherwise limited to the last 24 hours
LOCATION MONITORING
Geofeedia will continuously monitor and record social media from user defined locations providing the ability to perform historical searches and analysis, Unlimited number of location recordings and ability to change locations at any time
STREAMING
View up to five concurrent live streams of social media per licensed user
USER TRACK
Connect undercover Twitter and Instagram accounts and follow specific users posts
ARCHIVE AND EXPORT
Unlimited monitored Geofeeds and archival in secure data warehouse, Export Geofeed data to CSV format
ANALYTICS
Filtering by timeframe, keyword and user; trend views by volume, media, keyword and user; detailed view of feed items and associated metadata; curate items in collections
ALERTS
Create unlimited email alert notifications triggered by specific keywords, phrases or users, Customize Alerts at any time
LANGUATE TRANSLATION
Translate all content to and from more than 40 different languages
HOSTING AND STORAGE
Included
USER LICENSES AND DATA CHARGES
Unlimited number of user licenses (internal BRIC use only), Data includes up to 200,000 items per month >>

On hold, needs contract. nw 1/14/15

A0106

# City of Boston
# Purchase Order



## City of Boston

Purchasing Department
One City Hall
Room 808
Boston MA 02201
United States

| Dispatched | | |
|---|---|---|
| **Purchase Order** | **Date** | **Revision** |
| BOSTN-0000652357 | 2015-01-13 | |
| **Payment Terms** | **Freight Terms** | |
| 00 | DES PPD | |
| **Buyer** | | |
| Habershaw,Deirdre | | |

**Vendor:** 0000078005
Geofeedia, Inc.
444 N. Wells St. Suite 502
Chicago IL 60654
United States

**Bill To:** Auditing Department
One City Hall
Room M-4
Boston MA 02201
United States

**Ship To:** BPD New Police Headquarters
One Schroeder Plaza
Roxbury MA 02120
United States
**Attention:** See Detail Below

**Tax Exempt?** Y **State Tax Exempt ID:** 04-6001380

| Line-Sch | Item/Description | Quantity | UOM | PO Price | Extended Amt | Due Date |
|---|---|---|---|---|---|---|
| | | | | **Total PO Amount** | 9999.00 | |

******The above Purchase Order number must be included on all invoices to ensure accurate and timely payment.******

Official Approvals

| I certify that all records regarding this procurement are on file | Approved as to availability of appropriation | |
|---|---|---|
| Deirdre Habershaw | Sally Glora | 1/16/2015 |
| Department Head/Purchasing Agent/BPS Business Manager | City Auditor/BPS Business Manager | |

This is not a valid purchase order without the above signatures.

# City of Boston
# Purchase Order



## City of Boston

Purchasing Department
One City Hall
Room 808
Boston MA 02201
United States

| **Dispatched** | | |
|---|---|---|
| **Purchase Order** | **Date** | **Revision** |
| BOSTN-0000663364 | 2015-12-29 | |
| **Payment Terms** | **Freight Terms** | |
| 00 | DES PPD | |
| **Buyer** | | |
| Habershaw,Deirdre | | |

**Vendor:** 0000078005
Geofeedia, Inc.
444 N. Wells St. Suite 502
Chicago IL 60654
United States

**Bill To:** Auditing Department
One City Hall
Room M-4
Boston MA 02201
United States

**Ship To:** BPD New Police Headquarters
One Schroeder Plaza
Roxbury MA 02120
United States
**Attention:** See Detail Below

**Tax Exempt?** Y **State Tax Exempt ID:** 04-6001380

| Line-Sch | Item/Description | Quantity | UOM | PO Price | Extended Amt | Due Date |
|---|---|---|---|---|---|---|
| 1 - 1 | Geofeedia Standard Service Package for Boston Regional Intelligence Center - 2/1/16 through 5/31/16 | 1.00 | EA | 6700.00 | 6700.00 | 01/03/2016 |
| | Attention: David Carabin-BRIC | | | | | |
| 52907-200-211100-508F-2304-2015-HLS15002 | | 1.00 | | | | |

**Total PO Amount** 6700.00

******The above Purchase Order number must be included on all invoices to ensure accurate and timely payment.******

Official Approvals

| I certify that all records regarding this procurement are on file | Approved as to availability of appropriation | |
|---|---|---|
| Deirdre Habershaw | Sally Glora | 12/29/2015 |
| Department Head/Purchasing Agent/BPS Business Manager | City Auditor/BPS Business Manager | |

This is not a valid purchase order without the above signatures.

# OEM Equipment and Supply Pre-Requisition Form

## Requestor Information

| | | | |
|---|---|---|---|
| **Name** | David Carabin | **Discipline** | 508 Law Enforcement |
| **Phone** | 617-343-2748 | ***If other, please indicate*** | |
| **Email (below)** | | **Department/City/Town Name** | 211100 Boston Police |
| david.carabin@pd.boston.gov | | ***If other, please indicate*** | |

[

| Item Description | AEL # (required) | Quantity | Unit Price | Extended Price |
|---|---|---|---|---|
| Geofeedia Social Media Situational Awareness Service | N/A | 1 | $ 9,999.00 | $ 9,999.00 |
| | | | | $ - |
| | | | | $ - |
| | | | | $ - |
| | | | | $ - |
| | | | | $ - |
| **Total** | | | | $ 9,999.00 |

## Specifications

| | | | | | |
|---|---|---|---|---|---|
| **Manufacturer** | | **Make** | | **Model #** | |
| **Part #** | | **Style** | | **Color** | |
| **Size** | | **Useful life** | | **Licensing Required?** | N |
| **Suggested Vendor** | | Geofeedia | | | |
| **Other Information** | | | | | |

## Ship To

| | | | |
|---|---|---|---|
| **Name** | See above | **Department/City/Town Name** | 211100 Boston Police |
| **Phone** | | ***If other, please indicate*** | |
| **Street** | 1 Schroeder Plaza | **City/State/Zip** | Roxbury, MA |

## Jurisdiction Pont of Contact Signature & Date

**Signature** _____ **Date** 6/4/15

## City of Boston Use Only

**Request:** Appr / Rej: _____ **Date:** _____

## Header Defaults/PO Comments

| | | | | | |
|---|---|---|---|---|---|
| **GL Unit** | BOSTN | Account Code | 52907 | **Project/Grant** | UASI 13 (HLS14002) |
| **Fund** | 200 | **Dept ID** | 211100 Boston P | **Program (discipline)** | 508 Law Enforcement |
| **Location** | 4480 | **OEM Planner** | A. Murphy | **Program (equip type)** | F Logistical Support |
| **CFDA #** | 97.067 | **Bud Ref** | 0 | **Class (category)** | 23 Equipment |
| **PJ #** | U14-3.3 | AEL # | N/A | **Class (project)** | 04 Intelligence Capacity |

# OEM Equipment and Supply Pre-Requisition Form

## Requestor Information

| | | | |
|---|---|---|---|
| **Name** | David Carabin | **Discipline** | 508 Law Enforcement |
| **Phone** | 617-343-4388 | ***If other, please indicate*** | |
| **Email (below)** | | **Department/City/Town Name** | 211100 Boston Police |
| david.carabin@pd.boston.gov | | ***If other, please indicate*** | |

| Item Description | AEL # (required) | Quantity | Unit Price | Extended Price |
|---|---|---|---|---|
| Geofeedia service through 5/31/16 | N/A | 1 | $ 6,700.00 | $ 6,700.00 |
| | | | | $ - |
| | | | | $ - |
| | | | | $ - |
| | | | | $ - |
| | | | | $ - |
| **Total** | | | | $ 6,700.00 |

## Specifications

| | | | | | |
|---|---|---|---|---|---|
| **Manufacturer** | | **Make** | | **Model #** | |
| **Part #** | | **Style** | | **Color** | |
| **Size** | | **Useful life** | | **Licensing Required?** | N |
| **Suggested Vendor** | | SHI International | | | |
| **Other Information** | | | | | |

## Ship To

| | | | |
|---|---|---|---|
| **Name** | See Above | **Department/City/Town Name** | 211100 Boston Police |
| **Phone** | | ***If other, please indicate*** | |
| **Street** | Schroeder Plaza | **City/State/Zip** | Roxbury, MA |

## Jurisdiction Pont of Contact Signature & Date

**Signature** _____ **Date** 11/12/14

## City of Boston Use Only

**Request:** Appr / Rej: _____ **Date:** _____

## Header Defaults/PO Comments

| | | | | | |
|---|---|---|---|---|---|
| **GL Unit** | BOSTN | Account Code | 52907 | **Project/Grant** | UASI 15 (HLS16002) |
| **Fund** | 200 | **Dept ID** | 211100 Boston P | **Program (discipline)** | 508 Law Enforcement |
| **Location** | 4480 | **OEM Planner** | A. Murphy | **Program (equip type)** | F Logistical Support |
| **CFDA #** | 97.067 | **Bud Ref** | 0 | **Class (category)** | 23 Equipment |
| **PJ #** | U15-3.3 | AEL # | N/A | **Class (project)** | 04 Intelligence Capacity |