REAL-TIME OPEN-SOURCE-BASED INVESTIGATIONS AND RESEARCH

9.01 PURPOSE

The purpose of this regulation is to establish policies and procedures for the use of real-time open sources in crime analysis, situational assessments, criminal intelligence, criminal investigations, and employment background investigations. The policies and procedures contained herein are not meant to address one particular form of real-time open source, but rather real-time open sources in general, as advances in technology will occur and new tools will emerge.

9.02 DEFINITIONS

A. Blog: A self-published diary or commentary on a particular topic that may allow visitors to post responses, reactions, or comments. The term is short for “weblog.”

B. Deconfliction: Recognition that two or more Pennsylvania State Police (PSP) personnel are using or intending to use similar online aliases within the same time period, and subsequently reporting this knowledge to the involved parties to prevent unexpected overlap.

C. Online Alias: An online identity encompassing identifiers, such as name and date of birth, differing from the PSP member’s/employee’s actual identifiers, that uses a non-governmental Internet Protocol (IP) address. An online alias may be used to monitor activity on real-time open-source sites or to engage in authorized online undercover activity.

D. Online Undercover Activity: The utilization of an online alias to engage in interactions with a person(s) via real-time open-source sites that may or may not be part of the public domain (e.g., friending a person on Facebook).

E. Page: The specific portion of a real-time open-source site where content is displayed and managed by an individual or individuals with administrator rights.

F. Post: Content an individual shares on a real-time open-source site, or the act of publishing content on a real-time open-source site.

G. Profile: Information that a user provides about himself or herself on a real-time open-source network.

H. Public Domain: Any Internet resource that is open and available to the community at large, unprotected by copyright or patent, and subject to appropriation by anyone.

I. Real-time Open Sources: Websites, applications, and web-based tools that allow the creation and exchange of user-generated content and allow for user participation. This includes, but is not limited to, social networking sites (e.g., Facebook, Google+), microblogging sites (e.g., Twitter, Nixle), photo- and video-sharing sites (e.g., Instagram, YouTube), wikis (e.g., Wikipedia), blogs, and news sites (e.g., Digg, Reddit).

J. Real-time Open-Source Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

K. Speech: Expression or communication of thoughts or opinions in spoken words or in writing, or by expressive conduct, symbolism, photographs, video, or related forms of communication.

L. Wiki: Web page(s) developed collaboratively by a community of users that allows any user to add and edit content.

9.03 UTILIZATION OF REAL-TIME OPEN SOURCES AS AN INVESTIGATIVE TOOL

A. Real-time open sources are a valuable source of investigative information to facilitate efforts to detect and prevent criminal activity. Department personnel may utilize real-time open sources and monitoring tools, access social networks, utilize online aliases, and conduct online undercover activity for valid law enforcement purposes, in strict compliance with the directives and instructions provided in this regulation. The following are commonly recognized, but not all-inclusive, “valid law enforcement purposes:”

1. Crime analysis and situational assessment reports.

2. Criminal investigations.

3. Employment background investigations.

4. Development of criminal intelligence.

NOTE: Personnel shall be cognizant that the use of a personal Internet Service Provider to conduct Department business may compromise an investigation and/or disclose the true identity of the user. Additionally, the use of the Department's Enterprise Network to conduct a covert investigation may negatively impact the investigation. Therefore, personnel shall always consider the risks associated with using such online accounts and networks when conducting investigations and, when warranted, consider alternatives.

B. Department personnel shall use real-time open sources only to seek or retain information when the information meets one or more of the following criteria:

1. Concerns an individual, group, or organization reasonably suspected of criminal activity where such criminal activity would give rise to prosecution for a state offense graded a misdemeanor or felony, or for a federal offense for which the penalty is imprisonment for more than one year.

2. Is reasonably suspected to relate to an individual, group, or organization that is involved, or may be involved, in criminal activity, and the information is relevant to that activity.

3. Is useful in crime analysis or situational assessment reports.

4. Is evidence of criminal activity.

5. Is relevant to an employment background investigation.

C. Department personnel shall not utilize real-time open sources to seek or retain information based solely on:

1. An individual's, group's, or organization's participation in any political, religious, or social organization.

2. An individual's, group's, or organization's support of any nonviolent demonstration, assembly, protest, rally, or similar form of public speech.

D. Department personnel shall not directly or indirectly receive, seek, accept, or retain information from any individual or non-

government information provider who may receive a fee or benefit for providing such information, if it is known or there is reason to believe that:

1. The individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to the PSP.

2. The individual or information provider used methods for collecting the information that the PSP could not legally utilize.

3. The specific information sought from the individual or information provider could not legally be collected by the PSP.

4. The PSP has not taken the steps necessary to be authorized to collect the information.

9.04 AUTHORIZATION TO ACCESS REAL-TIME OPEN SOURCES AND/OR REAL-TIME OPEN-SOURCE NETWORKS

A. Public Domain:

1. Establishment of an online alias to access data in the public domain for investigative purposes requires approval of the immediate supervisor, or designee, of the requestor, and concurrence by the Supervisor, Operational Support Unit, Bureau of Criminal Investigation (BCI).

2. No supervisory approval is necessary to access data in the public domain for general research, topical information, or other law enforcement uses that do not require an online alias.

B. Online Aliases: An online alias shall only be used to seek or retain information that:

1. Concerns an individual, group, or organization reasonably suspected of criminal activity where such criminal activity would give rise to prosecution for a state offense graded a misdemeanor or felony, or for a federal offense for which the penalty is imprisonment for more than one year; or

2. Is reasonably suspected to relate to an individual, group, or organization that is involved, or may be involved, in criminal activity, and the information is relevant to that activity; or

3. Is useful in crime analysis or situational assessment reports.

9.05 AUTHORIZATION PROCEDURES FOR THE USE OF ONLINE ALIASES AND ONLINE UNDERCOVER ACTIVITY

A. Authorization for and Use of Online Aliases:

1. Personnel requiring an online alias shall complete and submit a Request to Conduct Real-Time Open-Source-Based Investigations, Form SP 5-605 (refer to Appendage A), to their immediate supervisor.

2. The immediate supervisor shall review and evaluate the request to determine whether there is a valid law enforcement purpose for the online alias, and whether the use of any proposed photographs, videos, drawings, and/or other similar items in association with the alias is legally acceptable. An example of what is not legally acceptable would include the use of a photograph of an individual without specific consent, or the use of copyrighted, trademarked, and/or service-marked information without the permission of the owner.

3. Upon completion of the review and evaluation of the request, the immediate supervisor shall endorse the Request to Conduct Real-Time Open-Source Investigations by indicating either “APPROVED” or “DENIED” and entering their initials in the Supervisor Review field. If the request is approved, the immediate supervisor shall forward the Request to Conduct Real-Time Open-Source Investigations to the Supervisor, Operational Support Unit, BCI, 1800 Elmerton Avenue, Harrisburg, Pennsylvania 17110, for concurrence. The online alias shall not be used until such concurrence is obtained.

4. Personnel with an approved online alias may use their online alias to make fictitious representations for

purposes of concealing their personal and professional identity and information in order to establish real-time open-source accounts (e.g., Facebook, Twitter, Instagram) for valid law enforcement purposes.

5. Any changes to an online alias, such as the URL, username, or ID, shall be immediately reported by submitting a revised Request to Conduct Real-Time Open-Source Investigations to the Supervisor, Operational Support Unit, BCI.

B. Authorization for Online Undercover Activity:

1. Personnel who have an authorized online alias may request authorization to engage in online undercover activity.

2. Online undercover activities shall only be conducted when there is reasonable suspicion to believe that a criminal offense has been, is being, or will be committed.

3. Personnel shall complete and submit a Request to Conduct Real-Time Open-Source Investigations to their immediate supervisor, or designee, prior to engaging in online undercover activities.

NOTE: Authorization is case specific and must be re-obtained whenever online undercover activity is utilized for a case or matter other than the case or matter for which authorization was originally obtained.

4. The immediate supervisor, or designee, shall review and evaluate the request to determine whether there is a valid law enforcement purpose for the online undercover activity, and whether such activity is appropriate. Upon completion of the review and evaluation of the request, the immediate supervisor, or designee, shall endorse the Request to Conduct Real-Time Open-Source Investigations by indicating either “APPROVED” or “DENIED” and entering their initials in the Supervisor Review field. The immediate supervisor, or designee, shall then forward the Request to Conduct Real-Time Open-Source Investigations to the appropriate Troop Criminal Investigation Section Commander or Division Director, who shall endorse the request by indicating either “APPROVED” or “DENIED” and entering their

initials in the Supervisor Review field, adjacent to the endorsement of the immediate supervisor, or designee. If the request is approved by both the immediate supervisor, or designee, and the appropriate Troop Criminal Investigation Section Commander or Division Director, the Request to Conduct Real-Time Open-Source Investigations shall be forwarded by the Troop Criminal Investigation Section Commander or Division Director, to the Supervisor, Operational Support Unit, BCI. The approved Request to Conduct Real-Time Open-Source Investigations shall be maintained in a secure database by the Operational Support Unit, BCI.

5. The requestor or the requestor's immediate supervisor shall provide notification of the termination of the online undercover activity by submitting a revised Request to Conduct Real-Time Open-Source Investigations to the Supervisor, Operational Support Unit, BCI. Upon receipt of the revised Request to Conduct Real-Time Open-Source Investigations, the Supervisor, Operational Support Unit, BCI, shall ensure the corresponding database record is updated accordingly.

C. Exigent Circumstances: When exigent circumstances exist, a supervisor, or designee, may provide verbal authorization for use of an online alias.

1. If verbal authorization for use of an online alias is granted, the supervisor, or designee, shall complete and submit a Request to Conduct Real-Time Open-Source Investigations to the appropriate Troop Criminal Investigation Section Commander or Division Director, or designee, within 24 hours of granting verbal authorization. The Request to Conduct Real-Time Open-Source Investigations shall explain the details of the request and a description of the exigent circumstances.

2. Immediately upon receipt of the Request to Conduct Real-Time Open-Source Investigations, the Troop Criminal Investigation Section Commander or Division Director, or designee, shall review the request and contact the Operational Support Unit, BCI, for deconfliction review.

9.06 DECONFLICTION

The Supervisor, Operational Support Unit, BCI, will administer the deconfliction program for all online undercover activity conducted by the Department. The Supervisor, Operational Support Unit, BCI, may deny or rescind the use of an online alias to prevent conflicts of use. The Operational Support Unit, BCI, will be responsible for receiving and entering data into the deconfliction system database and notifying affected Department personnel of identified conflicts.

9.07 UTILIZING REAL-TIME OPEN-SOURCE MONITORING TOOLS

A. Real-time open-source monitoring tools may be utilized in criminal investigations, development of criminal intelligence, crime analysis, threat assessments, and situational awareness reports. Real-time open-source monitoring tools may also be utilized to ensure the safety of the public at sporting events, demonstrations, or other large gatherings that require a law enforcement presence.

B. Real-time open-source monitoring tools acquired by the Department, and not in the public domain, shall only be used by personnel for official purposes.

9.08 SOURCE RELIABILITY AND CONTENT

Information developed from real-time open-source sites shall be corroborated using traditional investigative tools, including, but not limited to, interviews, verification of physical addresses, and verification of IP address information.

9.09 DOCUMENTATION AND RETENTION

A. All information obtained from real-time open-source sites shall be retained with the corresponding investigative report(s) in accordance with established retention procedures.

B. To the extent real-time open-source monitoring tools are utilized to manage incidents, including First Amendment-protected activities, the information obtained from the use of these tools shall be retained for a period of no more than 14 days.

EXCEPTION: Information obtained from real-time open-source monitoring tools that reveals a potential criminal nexus shall be

retained with the corresponding investigative report(s) for the incident in accordance with established retention procedures.

C. Information of a criminal nature obtained from a real-time open-source site may be captured by a variety of methods, including taking screen shots, printing chat logs, copying uniform resource locators, or storing the information via secure digital means.

9.10 UTILIZATION OF REAL-TIME OPEN SOURCES FOR EMPLOYMENT BACKGROUND INVESTIGATIONS

A. When conducting an employment background investigation, members may perform searches of real-time open-source sites and profiles in the public domain regarding a candidate.

B. Personnel shall not ask candidates to disclose passwords to real-time open-source sites or profiles. In the event a candidate discloses his/her password(s), personnel shall not use the password(s) to log into a candidate's real-time open-source site(s) or profile(s).

C. Personnel shall not collect or maintain information about the political, religious, or social views, associations, or activities of any individual or any group when conducting employment background investigations, unless such information directly relates to a candidate's suitability for employment.