Bureau of Counterterrorism

BCT Special Order 20-01

UTILIZATION OF SOCIAL MEDIA

ISSUE DATE:	02 September 2020	EFFECTIVE DATE:	02 September 2020
RESCINDS:	BOC SO 16-25; 13 May 16v		
INDEX CATEGORY:	**CNG/CTD/CMS**		

I. PURPOSE

This directive:

A. establishes the:

1. policy and procedures for social media investigations conducted by authorized members of the Bureau of Counterterrorism.

2. the Confidential Analytics Section within the Counterterrorism Division of the Bureau of Counterterrorism.

B. continues the Social Media Covert Identity Authorization (SMCID) form (CPD-41.307).

C. introduces the:

1. Consent to Assume Online Identity Authorization form (CPD-23.271).

2. Social Media SOMEX Team Intelligence Report (CPD-23.270).

3. Social Media Request form (CPD-23.171).

II. CONFIDENTIALITY

This directive is confidential and is for official use only. Department members are prohibited from disseminating, releasing, altering, defacing, or removing any record or information contained in this directive unless such action is required as part of their official duties.

III. LEGAL AUTHORITY

28 CFR Part 23: “Criminal Intelligence Systems Operating Procedures.”

IV. POLICY

A. Social Media provides an effective means for assisting authorized Bureau of Counterterrorism personnel in criminal investigations, intelligence development, and crime analysis. Use of social media will adhere to all applicable laws, Department directives, the Rules and Regulations of the Chicago Police Department, all information technology and records management policies, and this directive.

B. Authorized and on-duty Bureau of Counterterrorism personnel utilizing Department equipment or social media accounts and acting in an official capacity will **only** access and utilize social media for valid law enforcement purposes.

C. Any social media participation made pursuant to a Department member’s official duties are not considered protected speech under the First Amendment.

D. Members will adhere to Constitutional policing methods and respect the privacy, civil liberties, and the rights of community members.

E. Members must have reasonable articulable suspicion to collect and maintain intelligence data on an individual in accordance with 28 CFR Part 23.

V. DEFINITIONS

A. **Social Media –** any electronic communication through which participants utilize online communities to share information, ideas, private messages, and other content through an electronic format.

B. **Public Domain –** material which is available to the public, accessible through the internet for which no login information is necessary for online searches of information.

C. **Department Authorized Profile or Online Alias –** an online identity encompassing identifiers such as name and date of birth, differing from the member's actual identifiers that use a nongovernmental internet protocol (IP).

D. **Bona fides –** a process to develop an online person's legitimacy or credentials.

E. **In-Person Undercover Activity (IUA) –** for the purpose of this directive, undercover activity which occurs in person and is precipitated by the use of investigative online social media.

F. **Criminal Intelligence and 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 or organizations that are reasonably suspected of involvement in criminal activity.

G. **Online Undercover Activity (OUA) –** undercover activity which occurs when a member, utilizing a Department authorized profile or online alias, engages in building bona fide contacts with a person via social media sites that may or may not be in the public domain (e.g., "friending," for investigative purposes).

H. **Online Undercover Interaction (OUI) –** undercover activity which occurs when a member interacts or communicates with a person via social media sites that may or may not be in the public domain (e.g., posting comments, private messaging, etc.).

I. **Valid Law Enforcement Purpose –** the collection, use, retention, or sharing of information and intelligence gathered for the purpose of furthering 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 designated to protect the privacy, civil rights, and civil liberties of community members.

J. **Internet Protocol (IP) –** the method or protocol by which data is sent from one computer to another on the internet. Each computer (known as a host) on the internet has at least one IP address that uniquely identifies it from all other computers on the internet.

K. **Non-Attributable Equipment –** equipment that cannot be traced back to the Department or any other law enforcement agency.

L. **Reasonable Articulable Suspicion –** reasonable articulable suspicion is an objective legal standard that is less than probable cause but more substantiated than a hunch or general suspicion. Reasonable articulable suspicion depends on the totality of the circumstances which the sworn member observes and the reasonable inferences that are drawn based on the sworn member's training and experience. Reasonable articulable suspicion can result from a combination of particular facts, which may appear innocuous in and of themselves, but taken together amount to reasonable suspicion. Reasonable articulable suspicion should be founded on specific and objective facts or observations about how a suspect behaves, what the suspect is seen or heard doing, and the circumstances or situation in regard to the suspect that is either witnessed or known by the officer. Accordingly, reasonable articulable suspicion must be described with reference to facts or observations about a particular suspect's actions or the particular circumstances that an officer encounters. The physical characteristics of a suspect are never, by themselves, sufficient. Instead, those characteristics must be combined with other factors, including specific, non-general description matching the suspect or the observed behaviors of the suspect.

VI. AUTHORIZATION FOR USE OF SOCIAL MEDIA FOR INVESTIGATIVE PURPOSES

A. Only trained members assigned/detailed to the Criminal Network Group and related decentralized units and the Counterterrorism Division will be authorized to use social media for investigative purposes.

B. Any other Bureau of Counterterrorism unit outside the Criminal Network Group and the Counterterrorism Division tasked with monitoring social media as authorized by the Chief, Bureau of Counterterrorism, will adhere to applicable Department policy and any established unit-level procedures.

C. Division commanders will determine which members under his or her command will be approved to attend training for the use of social media for investigative purposes and intelligence gathering.

D. The Chief, Bureau of Counterterrorism, will determine which Bureau units or personnel are approved to conduct in-person undercover activity (IUA) as a result of a social media-related investigation.

VII. AUTHORIZED MANNER OF USE

A. Members will continue to follow any applicable Department directives including but not limited to **G09-01-03** "Use of the Internet," **G09-01-05** "Department-Issued Electronic Communication Devices," and **G09-01-06** "Use of Social Media Outlets," and "First Amendment and Police Actions" and its related addenda.

B. To maintain the longevity or active status of a created social media account or for the bona fides process, members may "follow" or "friend" groups or individuals without prior authorization. Any "following," "friending," or other social-media related activity related to a criminal investigation will require the proper authorization delineated in Item VIII-C of this directive.

C. Authorized Bureau of Counterterrorism personnel may utilize social media when:

1. the investigation is based upon a criminal predicate or threat to public safety;

2. reasonable articulable suspicion exits that an individual, regardless of citizenship or residency status, or criminal organization is involved in or is planning criminal activity that presents a threat to any individual or property;

3. such use can aide in crime analysis or situational assessment for public safety; and

4. intelligence gathered can be used to identify or interdict a gang-related conflict.

D. Social Media **will not** be used to seek or retain information about:

1. individuals or organizations solely on the basis of their religious, political, social views or activities;

2. an individual's participation in a particular non-criminal organization or lawful event unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual;

3. an individual's race, ethnicity, color, national origin, ancestry, religion, disability, gender, gender identity, sexual orientation, martial status, parental status, military discharge status, financial status, or lawful source of income, except that members may rely on the listed characteristics in a specific suspect description as delineated in the Department directive titled "Prohibition Regarding Racial Profiling and Other Bias Based Policing," or

4. an individual's age, other than to determine if someone is a minor.

E. Department authorized profiles and/or online alias accounts **will not** be accessed from equipment where an IP address can link the account to law enforcement.

F. Members **will not** use personal devices to search or seek out information pertaining to subjects or potential subjects of investigations.

G. Members **will not** create fictitious alias accounts from their personal devices or from Department equipment utilizing images downloaded from the internet.

H. Pictures and information utilized on Department authorized profiles and/or online alias accounts **must be** authorized by the exempt member approving the Social Media Covert Identity Authorization (SMCID) form (CPD-41.307). Members will ensure utilized pictures and information are not intellectual property.

VIII. PROCEDURES

A. Authorized Bureau of Counterterrorism personnel seeking to create a social media account for investigative purposes or intelligence gathering will complete and submit a Social Media Covert Identity Authorization (SMCID) form (CPD-41.307) through the appropriate chain of command to the Chief, Bureau of Counterterrorism. Furthermore:

1. all approved or rejected SMCID forms will be delivered via inter-office mail to the requesting member or the requesting member's unit of assignment or detail by Bureau of Counterterrorism, Office of the Chief, personnel.

2. Upon receipt of an approved SMCID form, the requesting member will **hand carry** the completed form to the Confidential Matters Section (CMS) at the Homan Square Facility (HSF).

NOTE: All user names will be appropriate and consistent with the core values of the Chicago Police Department.

B. Online activities that are **not** considered to be undercover in nature are permissible for trained and authorized members. These activities do not require documentation or supervisory approval. Examples of activities that are **not** considered to be undercover in nature include, but are not limited to:

1. internet searches of publically available information that would otherwise be available in the same manner that it is to the general public;

2. online resources that require registration for access provided the registration process is designated to accept all applications from the public and in no way creates a restriction as to who may access the information;

3. online resources that require a fee for access provided that anyone in the general public can purchase access to the same information;

4. accessing, viewing, or joining a public chat rooms, provided that:

   a. the chat room is configured to allow access to any member of the general public, and

   b. the member does not interact, under any circumstances, with any other member of the public chat.

5. joining an email list;

6. accessing and reading public social media postings;

7. "following" individuals and organizations on social media not related to an active investigation;

8. establishing internet "alerts."

C. Bureau of Counterterrorism personnel who have an authorized social media profile and are seeking to engage in online undercover activity (OUA) and/or an online undercover interaction (OUI) will request authorization to engage in such activity and/or interaction by submitting a formal written request to his or her division commander or designated exempt-ranking member. The division commander or designated exempt-ranking member will provide the requesting member with a formal written approval or rejection of the request. The requesting member will retain the original request and approval/rejection in the appropriate case file and copies of the original request and formal written approval/rejection will be **hand carried** to CMS.

NOTE: If exigent circumstances exist for an authorized social media profile to be used in online undercover activity and/or an online undercover interaction, the requesting member may receive verbal approval from his or her division commander or designated exempt-ranking member until until there is reasonable time to complete a formal written request. (e.g., pending violent crime).

D. Approved Bureau of Counterterrorism personnel who have an authorized social media profile and are seeking to engage in an in-person undercover activity (IUA) will request authorization to engage in such activity by submitting a formal written request to his or her division commander or designated exempt-ranking member. 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., online display of weapons, narcotic sales, armed robberies, murder for hire, etc.). The division commander or designated exempt-ranking member will provide the requesting member with a formal written approval or rejection of the request. The requesting member will retain the original request and approval/rejection in the appropriate case file and copies of the original request and formal written approval/rejection will be **hand carried** to CMS.

NOTE: If exigent circumstances exist for an authorized social media profile to be used for in-person undercover activity, the requesting member may receive verbal approval from his or her division commander or designated exempt-ranking member until there is reasonable time to complete a formal written request (e.g., pending violent crime).

E. If a victim, witness, or any other source during the course of an investigation consents for the investigating member to allow the Chicago Police Department full access to the accounts for the purpose of viewing its content, the Consent to Assume Online Identity Authorization form (CPD-23.271) will be completed. Upon completion, a copy will be added to the case file and the original inventoried via eTrack.

NOTE: Members who have assumed the online identity of a victim, witness, or any other source will not interact (post, comment, or respond to messages) posing as that victim, witness, or source. Once the investigation is completed or the individual revokes the consent, the utilizing member will no longer access the consenting individual's account(s).

F. Bureau of Counterterrorism personnel will:

1. conduct web-based investigative activity as well as utilize Department authorized profiles and/or online aliases in accordance with Item VII of this directive for the purpose of:

    a. collecting criminal intelligence;

    b. conducting and generating analytical assessments;

    c. identifying criminal activity or patterns of criminal activity;

    d. identifying witnesses or previously unknown offenders and/or victims; and

    e. identifying any other information and/or intelligence that may serve as a valid law enforcement purpose.

2. submit preservation requests with social media providers, as required;

3. ensure Chicago High Intensity Drug Trafficking Area (HIDTA) is notified and that the information regarding any social media account under investigation is submitted on a Chicago HIDTA Deconfliction Submission for event deconfliction in accordance with established procedures.

4. prepare and execute search warrants on electronic devices or providers or serve other legal processes to providers, as required.

5. prepare Officer Safety Alerts and/or Information Bulletins and disseminate to CPIC, as required or determined necessary;

6. coordinate with other Departmental units, outside agencies, and/or prosecuting offices, as required;

7. document all information obtained via a Social Media Exploitation (SOMEX) Team Intelligence Report (CPD-23.270).

G. Social Media Files Upon Reassignment or Detail

1. When a member is transferred or detailed out of an authorized unit, utilized social media accounts **must** be reassigned to another member assigned/detailed to an authorized unit or deactivated.

2. The reassignment or deactivation of a social media account will require the completion of a To-From-Subject report through the appropriate chain of command to the member's division commander. An approved To-From-Subject report will be submitted to the CMS and retained in the social media account file.

NOTE: Division commanders have the discretion to determine if an account should be reassigned or deactivated.

H. Equipment

1. During a covert investigation, only non-attributable equipment should be utilized.

2. Non-attributable equipment will be used strictly for covert activity and will not be used to access private/personal sites/email in true name or for Department use.

3. Data of evidentiary value captured on a covert device will be transferred only via compact disk (CD) or digital video disk (DVD) and must be entered into evidence via eTrack within 10 working days.

IX. REQUESTING ASSISTANCE FROM THE CONFIDENTIAL ANALYTICS SECTION

1. The Confidential Analytics Section (CAS), Counterterrorism Division, may assist bureau personnel with social media-related investigations or intelligence gathering.

2. To request the assistance of CAS, bureau members will:

a. complete the Social Media Request form (CPD-23.171) with supervisory approval, and

b. hand deliver the form to the CAS located at the HSF.

NOTE: In case of an emergency, bureau personnel may contact the CAS directly. An emergency that is occurring during non-operational hours, members will contact the designated CAS supervisor who will forward the request to the on-call CAS member to provide assistance.

X. REPORTING AND DISSEMINATING

A. Members initiating a social media investigation will complete the appropriate criminal or non-criminal case report.

B. Members will document information and intelligence received via social media sites on a Social Media Exploitation (SOMEX) Team Intelligence Report (CPD-23.270). Completed reports will be submitted to a supervisor for approval. Upon approval, original reports will be retained in the proper file corresponding to the request. Copies of the original reports will be disseminated to a unit supervisor for which the intelligence relates, for inclusion into the official case file, if it is not the documenting member's case.

NOTE: Members will not distribute reports outside the Chicago Police Department unless an Inquiry Request Worksheet (CPD-11.704) is submitted and approved by supervisor in accordance with the Department directive **G09-01-01** "Access to Computerized Data, Dissemination, and Retention of Computer Data."

C. Members will follow **G09-01-01** "Access to Computerized Data, Dissemination, and Retention of Computerized Data and Item XI of this directive concerning the review and purging electronic criminal intelligence information.

D. Members will report the contents of stored electronic messages, such as emails, which contain applicable content applicable to investigative activity. These retained electronic communications will be incorporated into case documents for court discovery purposes.

E. If a Department member observes information that cannot be printed due to the short duration the information is available (e.g., Snapchat), the member will document any information of investigatory value in an investigatory report.

IX. CONFIDENTIAL MATTERS SECTION

The Confidential Matters Section (CMS) will:

A. conduct an annual audit of all utilized social media accounts.

B. review all submitted SMCID forms for completeness.

C. maintain social media account files including:

1. submitted SMCID forms.

2. Copies of the original requests and formal written approvals/rejection from the Bureau of Counterterrorism command staff personnel authorizing members to engage online undercover activity (OUA), online undercover interaction (OUI), and in-person undercover activity (IUA).

3. the approved To-From-Subject report for the reassignment or deactivation of social media account upon the utilizing member's reassignment or detail.

XI. RECORD RETENTION

All reports generated under this directive will be retained in accordance with existing Department retention directives and existing record preservation orders.

Related Directives:

- G02-02 "The First Amendment and Police Action" and addenda.
- G02-04 "Prohibition Regarding Racial Profiling and Other Bias Based Policing
- G09-01-01 "Access to Computerized Data, Dissemination and Retention of Computer Data"
- G09-01-03 "Use of the Internet"
- G09-01-05 "Department-Issued Electronic Communication Devices"
- G09-01-06 "Use of Social Media Outlets"

Jose M. Tirado
Chief
Bureau of Counterterrorism

T20-012 JB/RCL