Confidential Analytics Section

Social Media Investigations – Policies, Part 1

2020

G02-02

The First Amendment and Police Actions

II. POLICY

It is the policy of the Chicago Police Department to conduct all investigations for ***a proper law enforcement purpose***. Each and every investigation must safeguard the constitutional liberties of all persons. Police conduct which may affect the exercise of First Amendment rights will be conducted in accordance with this directive. Department members may not investigate, prosecute, disrupt, interfere with, harass, or discriminate against any person engaged in First Amendment conduct ***for the purpose of punishing, retaliating, or preventing the person from exercising his or her First Amendment rights***.

G02-02
The First Amendment and Police Actions

IV. FIRST AMENDMENT RIGHTS UPON THE PUBLIC WAY

A. The public way generally includes public property held open to the public such as city parks, public streets, and sidewalks. The public way ***does not include privately-owned property, such as the United Center, and publicly-owned property not open to the public, such as the working area of a police facility***.

B. Persons on the public way have the right to:
   1. ***express their views through any form of communication***, including distribution or sale of newspapers, magazines, handbills or other printed matter; and
   2. **solicit financial contributions**.

G02-02
The First Amendment and Police Actions

IV. FIRST AMENDMENT RIGHTS UPON THE PUBLIC WAY (cont)

C. The rights protected by the First Amendment and exercised on the public way are ***not absolute and are subject to time, place, and manner restrictions***, as well as any and all other applicable laws.

EXAMPLE:
Persons expressing views protected by the First Amendment on the public way are required to comply with laws ***prohibiting physical obstruction of the movement of persons and vehicles on the public way or place, and damage to public or private property.***

G02-02
The First Amendment and Police Actions

IV. FIRST AMENDMENT RIGHTS UPON THE PUBLIC WAY (cont)

D. Persons on the public way may ***freely distribute, without charge*** to others, material or messages containing First Amendment protected ideas.

E. Speech Peddling: Persons Selling a Protected Message

1. Section 4-244-141 of the Municipal Code of Chicago (MCC) defines speech peddling as a licensed ***peddler who sells or exchanges for value*** anything containing words, printing, or pictures that predominantly communicate a non-commercial message.

1. Persons engaged in speech peddling ***are subject to geographic restrictions and permit requirements*** contained in the MCC. For example, no person shall be allowed to engage in speech peddling within the Central District without a speech peddling permit (4-244-141 (b) MCC).

G02-02-01

Investigations Directed at First Amendment – Related Information

II. FIRST AMENDMENT POLICY

A. Proper and Permissible Police Action

2. All police action will be conducted for a ***reasonable law enforcement purpose***.

b. A reasonable law enforcement purpose means that the investigation is ***intended to address unlawful conduct, either past, present, or future, including whether a person has knowledge of such past, present, or future unlawful conduct, or to address public safety issues, whether they amount to criminal conduct or not. A reasonable law enforcement purpose would include acquiring information or intelligence which may be useful in allocating resources for public safety and acquiring information or intelligence which may be useful for future criminal investigations.***

G02-02-01

Investigations Directed at First Amendment – Related Information

II. FIRST AMENDMENT POLICY

B. Prohibited Action: Under no circumstances will any sworn member or other employee of the Chicago Police Department:

1. investigate, prosecute, disrupt, interfere with, or harass any person ***for the purpose of preventing*** that person from engaging in conduct protected by the First Amendment;

2. investigate, prosecute, disrupt, interfere with, or harass any person ***for the purpose of punishing or retaliating*** against that person for engaging in conduct protected by the First Amendment;

3. ***discriminate against any person on the basis*** of conduct protected by the First Amendment, except as may be permitted by law;

4. ***authorize, assist, or encourage*** any person to engage in conduct which violates Items II-B-1 through II-B-3.

G02-02-01

Investigations Directed at First Amendment – Related Information

III. IMPERMISSIBLE INVESTIGATIONS

A. It is not permissible to investigate someone ***solely*** because that person ***advocates a position in his or her speech or writings which is offensive or disagreeable***. It is not permissible to investigate someone for the content of his or her speech if there is no reasonable law enforcement purpose, such as ***criminal conduct or public safety***.

G02-02-01

Investigations Directed at First Amendment – Related Information

III. IMPERMISSIBLE INVESTIGATIONS

B. Examples of Investigations Which Violate the First Amendment

1. A police officer undertakes an investigation of a crime allegedly committed by a member of a race-based hate group. During the course of the investigation, the officer decides to interview the employer of an admitted member of the group, even though there is no indication that the employer has any knowledge of the crime. The officer conducts the interview ***because he feels that the employer should be aware that one of his employees is a member of this type of organization***. Although the investigation into the crime is permissible, ***there is no appropriate law enforcement justification for the interview with the employer***, and therefore, it violates the First Amendment.

G02-02-01

Investigations Directed at First Amendment – Related Information

III. IMPERMISSIBLE INVESTIGATIONS

B. Examples of Investigations Which Violate the First Amendment

2. A police officer hears a CD which contains numerous songs with lyrics derogatory towards law enforcement, but none of the songs threaten violence. The officer decides to investigate the musical group ***because the officer is offended by the lyrics***. The officer talks to the group's producer, manager, and record label about why the group puts out music with such lyrics. ***There is no appropriate law enforcement justification for this investigation***, and therefore, it violates the First Amendment and is impermissible.

G02-02-01

Investigations Directed at First Amendment – Related Information

IV. PERMISSIBLE INVESTIGATIONS WHICH REQUIRE NO SPECIAL AUTHORIZATION

A. Investigations not based on First Amendment activity are permissible and require no special authorization under this directive. If an investigation is ***begun based on an articulable suspicion of criminal activity*** this directive ***does not require special authorization for that investigation even if at some point it involves examination of speech or other expression***. However, such an investigation will still comply with the First Amendment policy as set forth in Item II of this directive.

C. Investigating Hate Crimes Within the Confines of the First Amendment

…the ***investigation is initiated due to the crime***, and the review of expression is permissible as having a reasonable purpose related to the elements of the crime.

G02-02-01

Investigations Directed at First Amendment – Related Information

IV. PERMISSIBLE INVESTIGATIONS WHICH REQUIRE NO SPECIAL AUTHORIZATION

B. Examples of Permissible Investigations Which Require No Special Authorization

1. An officer receives information that a suspect is selling marijuana at a particular location. The officer goes undercover to purchase marijuana from the suspect in order to gather evidence to prosecute the suspect criminally. During the drug transaction, the suspect mentions that he thinks marijuana should be legal in the United States. ***The investigation was undertaken due to the reasonable suspicion that the suspect was selling drugs,*** not as a result of his speech or opinion. Therefore, this directive does not require special authorization for the investigation

G02-02-01

Investigations Directed at First Amendment – Related Information

IV. PERMISSIBLE INVESTIGATIONS WHICH REQUIRE NO SPECIAL AUTHORIZATION

B. Examples of Permissible Investigations Which Require No Special Authorization

2. An officer has arrested several members of a street gang for violent criminal conduct. The officer wants to ***identify regular associates of these gang members, including searching the Internet for evidence of the gang member's associates***. This investigation is based upon ***reasonable suspicion that the associates of these gang members are engaging in illegal conduct*** and is not based upon speech or other expression. Therefore, no special authorization is required.

G02-02-01

Investigations Directed at First Amendment – Related Information

IV. PERMISSIBLE INVESTIGATIONS WHICH REQUIRE NO SPECIAL AUTHORIZATION

B. Examples of Permissible Investigations Which Require No Special Authorization

4. An informant tells an officer that an anarchist ***group plans to deface the building*** of a large corporate headquarters located in downtown Chicago. Based upon this information, the officer begins an investigation of this group, ***including a review of the Internet sites and any writings of the group, to determine the credibility and any details of the alleged plot***. This investigation is based upon a ***reasonable suspicion of criminal conduct***, rather than the oral or written expressions of the group. Therefore, no special authorization is required.

G02-02-01

Investigations Directed at First Amendment – Related Information

V. PERMISSIBLE INVESTIGATIONS REQUIRING SPECIAL AUTHORIZATION

A. First Amendment Information Gathering Investigation Defined
A First Amendment information gathering investigation is ***the gathering and analysis of written or oral speech or other expression*** which is undertaken:

1. due to or ***on the basis of the content*** of the speech or other expression ***and***;

2. for the purpose of ***preventing crime or for the purpose of aiding likely future investigations, even in the absence of an articulable suspicion to believe that a violation of law has occurred***.

G02-02-01

Investigations Directed at First Amendment – Related Information

V. PERMISSIBLE INVESTIGATIONS REQUIRING SPECIAL AUTHORIZATION

B. First Amendment Information Gathering Policy

1. Certain law enforcement investigations ***prompted by or based upon a person's speech or other expression, whether written or oral, are permitted provided that there is a reasonable law enforcement purpose***, as detailed in Item II-A-2 of this directive, for doing so. If an investigation is prompted by or based upon a person's speech or other expression and will be conducted for a reasonable law enforcement purpose, the investigation is permissible but requires special authorization as outlined in Item II of the Special Order entitled "Investigations Directed at First Amendment-Related Information."

G02-02-01

Investigations Directed at First Amendment – Related Information

V. PERMISSIBLE INVESTIGATIONS REQUIRING SPECIAL AUTHORIZATION

B. First Amendment Information Gathering Policy

2. It is permissible to gather information consisting of speech or other expression that is ***expected to serve a reasonable law enforcement purpose in the future even if not based on an articulable suspicion that a violation of law has occurred***, and even when the investigation is undertaken on the basis of speech or other conduct protected by the First Amendment. ***Information gathering is a legitimate law enforcement function provided it is conducted for reasonable law enforcement purposes, such as preventing crimes or providing information that may constitute useful future investigative leads.***

G02-02-01

Investigations Directed at First Amendment – Related Information

V. PERMISSIBLE INVESTIGATIONS REQUIRING SPECIAL AUTHORIZATION

B. First Amendment Information Gathering Policy

3. Advocacy of violence or unlawful acts or expression of sympathy with violence or unlawful acts is protected by the First Amendment until such advocacy presents an imminent and credible threat. ***Nevertheless, law enforcement has a duty to gather information about groups and individuals who advocate law breaking or express sympathy with law breaking in order to determine whether these groups or individuals are engaged in or plan unlawful activities, as well as to obtain information that may be useful in future investigations and preventing crime.***

G02-02-01

C. Examples of First Amendment Information Gathering Investigations Permitted if Specially Authorized

1. A person is standing on a street corner in the Loop, violating no laws, but is offering passers-by literature supporting the bombing of targets in the United States. (An investigation) ***to determine the source's intentions, capabilities, funding, and other information related to assessing future violence***.
2. A police officer discovers a site on the internet run by a hate group which espouses violence against government officials and lists the addresses and personal routines of certain government officials. The officer opens an investigation…***undertaken to determine the credibility of any threats and the future criminal plans of the hate group***.
3. A public rally is planned. One of the groups urging its members to attend is also speaking about the need to target and destroy certain symbols of corporate America. (An investigation) ***to determine if any and what criminal activity is planned for the rally is a reasonable law enforcement purpose.***

S02-02-01

Investigations Directed at First Amendment – Related Information

A. Approvals and Authorization

First Amendment-Related Investigation Initiation Report - ***To/From to exempt member addressed to "Superintendent of Police Attention: General Counsel"***

a. Date and time the investigation will be initiated;

b. Basis of initiating the investigation and the reasonable law enforcement purpose of the investigation;

c. Methods of investigation sought to be employed and why these methods are likely to be more effective than less invasive investigative methods;

d. Amount of time the investigation is expected to last.

S02-02-01

Investigations Directed at First Amendment – Related Information

A. Approvals and Authorization (cont.)

1. Exempt commanding officer- complete First Amendment worksheet (CPD-11.44) and submit To-From-Subject report to Bureau Chief;

2. Bureau Chief- submit First Amendment worksheet (CPD-11.44) and submit To-From-Subject report to General Counsel for concurrence;

3. General Counsel for Concurrence- If non-concurred, First Deputy Superintendent makes decision.

S02-02-01

Investigations Directed at First Amendment – Related Information

A. Approvals and Authorization (cont.)

5. Notwithstanding the requirement of special authorization, a member may initiate and conduct a First Amendment-related information gathering investigation ***without prior special authorization, provided***:

   a. it is ***impractical*** to submit the required paperwork prior to initiating the investigation;

   b. an exempt commanding officer has ***verbally approved the investigation***, however, the use of an infiltrator may be approved verbally only by the Superintendent; and,

   c. all required paperwork is submitted as soon as practicable but ***in no event later than twenty-four (24) hours after the initiation of the investigation***.

S02-02-01

Investigations Directed at First Amendment – Related Information

B. Additional Authorization Necessary For Use of Infiltrator

Any use of an infiltrator requires the prior approval of the Superintendent. A request to use an infiltrator will be submitted in a separate To-From-Subject report in the form of a First Amendment-related investigation initiation report, in accordance with the requirements of such a report as indicated in Item II-A-1 of this directive, with an additional approval line for the Superintendent.

S02-02-01

Investigations Directed at First Amendment – Related Information

C. Continued Monitoring

Members will ***continually assess*** the authorized use of undercover methods and determine whether the use of these methods remain warranted in light of the information generated by these methods. ***Members conducting the investigation will submit to their exempt commanding officer To-From-Subject reports detailing the progress of the investigation at thirty-day (30) intervals or at shorter intervals as directed by the exempt commanding officer***. The exempt commanding officer may revoke his or her approval at any time for good reason and will, upon such revocation, notify his or her chief. A chief may revoke his or her approval at any time for good reason. Upon the revocation of either approval, the investigation will be terminated.

S02-02-01

Investigations Directed at First Amendment – Related Information

C. Time Limits on Authorizations of Investigations

1. Authorization ***to conduct*** First Amendment-related information gathering will be in effect for a period ***not to exceed one hundred twenty (120) days***
2. Authorization to employ ***undercover methods*** will be in effect for a period not to exceed thirty (30) days
3. Continued use of ***an infiltrator*** after the expiration of the initial authorized period also requires application for an ***extension for up to thirty (30) days***
4. All members involved in the investigation will be notified of the termination, and ***all documents will be retained and/or forwarded as required***.

S02-02-01

Investigations Directed at First Amendment – Related Information

III. Public Gatherings and 1st Amendment Conduct

A. Documenting Investigations of Public Gatherings

Information obtained during the course of such a preliminary investigation will be made the subject of an ***Automated Information Report***, in order to facilitate future assessments of resources and public safety. That report, along with ***pertinent attachments, will be forwarded through the chain of command to the chief of the bureau of the member and to the First Deputy Superintendent***. The Automated Information Report will be treated, maintained, and retained in accordance with Department policy for non-First Amendment-related investigations.

S02-02-01

Investigations Directed at First Amendment – Related Information

III. Public Gatherings and 1st Amendment Conduct (cont)

B. Video Recording, Audio Recording, and Photographing Public Gatherings

Video recording and photographing of events on the public way are ***generally appropriate and may be conducted for any proper law enforcement purpose***, including documenting violations of law, monitoring police conduct, defending against allegations of police misconduct, aiding in the future coordination and deployment of police resources, and training. Furthermore, audio recording may be authorized at the discretion of an exempt commanding officer as circumstances warrant, including documenting the issuance of police orders, warnings, or notices.

S02-02-01

Investigations Directed at First Amendment – Related Information

III. Public Gatherings and 1st Amendment Conduct

B. Video Recording, Audio Recording, and Photographing Public Gatherings (cont)

If done for any of the above reasons, video recording, audio recording, or photographing a public gathering is not an investigation directed toward First Amendment-related information within the meaning of this directive, and the retention and disposal of such video recording, audio recording, or photographs will follow the restrictions outlined

If video recording, audio recording, or photographing is done as part of an First Amendment-related information gathering investigation, the retention and disposal of such video recordings, audio recording, or photographs will follow the restrictions outlined

S02-02-01

Investigations Directed at First Amendment – Related Information

Retention of Video Recordings, Audio Recordings, or Photographs Taken at Public Gatherings

As soon as practicable, the unit which conducted the video recording, audio recording, or photographing will send a To-From-Subject report to the persons listed below, indicating the nature of the video recording, audio recording, or photographs, ***the fact that they will be held within the unit for ninety (90) days, and requesting a written signature acknowledging that there is no known reason to retain them past the ninety-day time period***.

- Office of the General Counsel
- Chief, Bureau of Detectives
- Deputy Chief, Education and Training Division
- Chief, Bureau of Organizational Development
- Commander, Special Events Unit
- Chief Administrator, Civilian Office of Police Accountability

S02-02-01

Investigations Directed at First Amendment – Related Information

Retention of Video Recordings, Audio Recordings, or Photographs Taken at Public Gatherings

If the persons listed above all sign an acknowledgment that there is no known reason to retain the video recording, audio recording, or photographs, then the unit retaining the video recording, audio recording, or photographs will ***dispose of them but retain the signed acknowledgments in unit files***. If any person listed in Item III-B-4-a-(1) through (6) requests that the video recording, audio recording, or photographs be retained due to future training or planning purposes or due to allegations of criminal conduct or officer misconduct arising out of the event, then the person requesting retention will direct the unit where to send the video recording, audio recording, or photographs. The sending unit will document the transfer of the video recording, audio recording, or photographs in a ***To-From-Subject report, which will be signed by a member at the accepting unit*** to indicate receipt of the video recording, audio recording, or photographs. ***The To-From-Subject report will be retained in original unit files***.

S02-02-01

Investigations Directed at First Amendment – Related Information

Retention of Documents

The exempt commanding officer of the investigating unit will retain the documents, video recordings, audio recordings, or photographs related to a First Amendment-related information gathering investigation.

BCT SO 20-01
Utilization of Social Media

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

B. continues the Social Media Request form (CPD-11.310).

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).

BCT SO 20-01
Utilization of Social Media

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.

BCT SO 20-01
Utilization of Social Media

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.

BCT SO 20-01
Utilization of Social Media

V. DEFINITIONS (cont)

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.).

BCT SO 20-01
Utilization of Social Media

V. DEFINITIONS (cont)

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.

BCT SO 20-01
Utilization of Social Media

V. DEFINITIONS (cont)

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.

BCT SO 20-01
Utilization of Social Media

VI. AUTHORIZATION FOR USE OF SOCIAL MEDIA

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.

BCT SO 20-01
Utilization of Social Media

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.

BCT SO 20-01
Utilization of Social Media

VII. AUTHORIZED MANNER OF USE (cont)

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 exists 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.

BCT SO 20-01
Utilization of Social Media

VII. AUTHORIZED MANNER OF USE (cont)

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

BCT SO 20-01
Utilization of Social Media

VII. AUTHORIZED MANNER OF USE (cont)

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 (e.g., *using attributable equipment which is connected to the Department's network)*
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 initial 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.

BCT SO 20-01
Utilization of Social Media

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.

BCT SO 20-01
Utilization of Social Media

VIII. PROCEDURES (cont)

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;

BCT SO 20-01
Utilization of Social Media

VIII. PROCEDURES (cont)

4. accessing, viewing, or joining a public chat rooms, provided that:
    a. a. the chat room is configured to allow access to any member of the general public, and
    b. 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."

BCT SO 20-01
Utilization of Social Media

VIII. PROCEDURES (cont)

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 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).

BCT SO 20-01
Utilization of Social Media

VIII. PROCEDURES (cont)

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).

BCT SO 20-01
Utilization of Social Media

VIII. PROCEDURES (cont)

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 an individual ***WILL NOT interact*** (post, comment, respond to messages) posing as that individual. Once the investigation is completed or the individual revokes consent, the utilizing member will no longer access the consenting individual's account(s).

BCT SO 20-01
Utilization of Social Media

VIII. PROCEDURES (cont)

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.

BCT SO 20-01
Utilization of Social Media

VIII. PROCEDURES (cont)

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).

BCT SO 20-01
Utilization of Social Media

VIII. PROCEDURES (cont)

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.

BCT SO 20-01
Utilization of Social Media

VIII. PROCEDURES (cont)

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***.

BCT SO 20-01
Utilization of Social Media

IX. REQ ASSISTANCE FROM THE CONFID 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.

BCT SO 20-01
Utilization of Social Media

X. REPORTING AND DISSEMINATING

A. ***Members initiating a social media investigation will complete the appropriate report, including a Social Media Intelligence Report-BCT (CPD-41.310), when applicable.***

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."

BCT SO 20-01
Utilization of Social Media

X. REPORTING AND DISSEMINATING

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 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.

BCT SO 20-01
Utilization of Social Media

XI. CONFIDENTIAL MATTERS SECTION

The Confidential Matters Section (CMS) will:

A. conduct an ***annual audit*** of all utilized social media accounts ***for the Department***.

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.

BCT SO 20-01
Utilization of Social Media

XI. RECORD RETENTION

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

HIDTA DECONFLICTION

WHAT IS HIDTA

A. High Intensity Drug Trafficking Areas (HIDTA) program

B. Congress created the HIDTA program through the Anti-Drug Abuse Act of 1988

C. The program aims to reduce drug production and trafficking through four means:

   1. promoting coordination and information sharing between federal, state, local, and tribal law enforcement;
   2. bolstering intelligence sharing between federal, state, local, and tribal law enforcement;
   3. providing reliable intelligence to law enforcement agencies such that they may be better equipped to design effective enforcement operations and strategies; and
   4. promoting coordinated law enforcement strategies that rely upon available resources to reduce illegal drug supplies not only in a given area, but throughout the country.

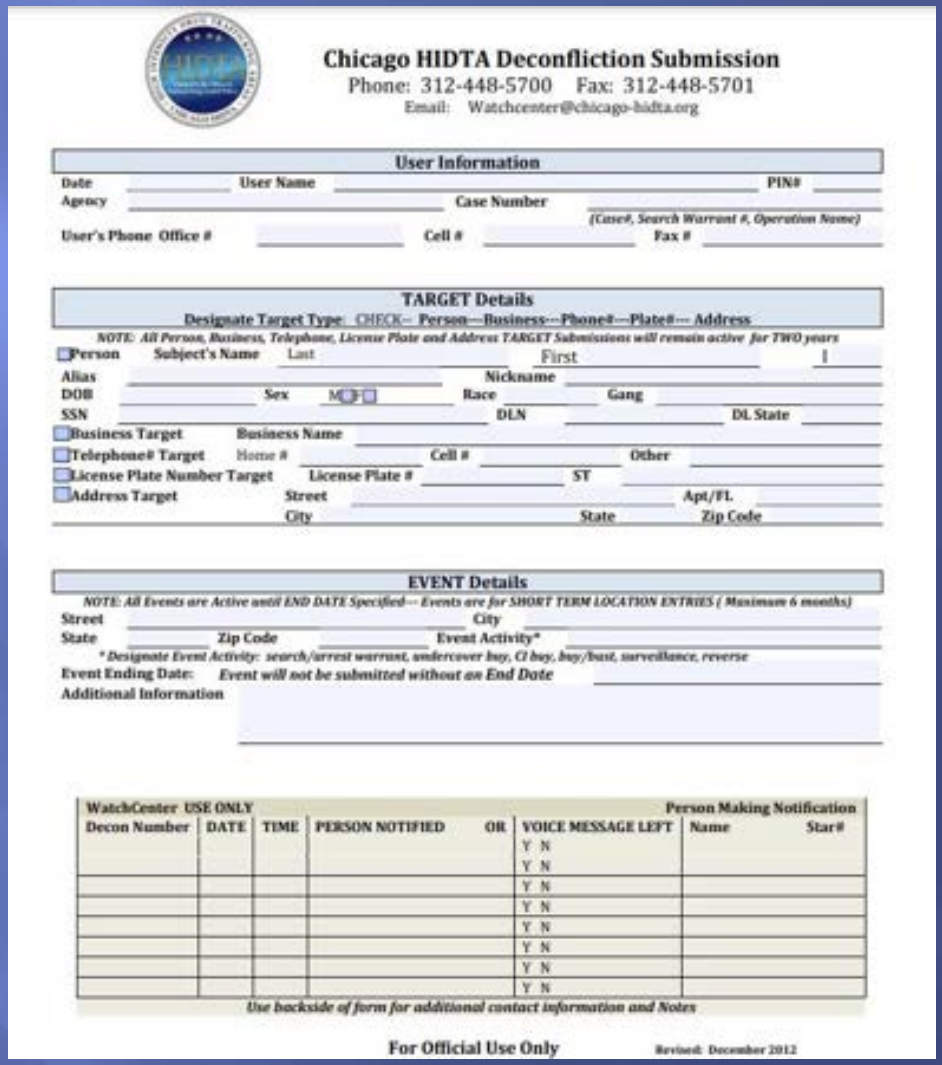
HIDTA DECONFLICTION

WHAT IS EVENT DECONFLICTION?

Event deconfliction is the process of determining when law enforcement personnel are conducting an event in close proximity to one another at the same time.

Events include law enforcement actions, such as undercover operations, surveillance, and executing search warrants.

When certain elements (e.g., time, date, location) are matched between two or more events, a conflict results. Immediate notification is made to the affected agencies or personnel regarding the identified conflict.



Chicago HIDTA Deconfliction Submission

Phone: 312-448-5700 Fax: 312-448-5701
Email: Watchcenter@chicago-hidta.org

User Information

Date _____ User Name _____ PIN# _____
Agency _____ Case Number _____
(Case#, Search Warrant #, Operation Name)
User's Phone Office # _____ Cell # _____ Fax # _____

TARGET Details

Designate Target Type: CHECK-- Person---Business---Phone#---Plate#--- Address

NOTE: All Person, Business, Telephone, License Plate and Address TARGET Submissions will remain active for TWO years

☐ Person Subject's Name Last _____ First _____ I _____
Alias _____ Nickname _____
DOB _____ Sex M F _____ Race _____ Gang _____
SSN _____ DLN _____ DL State _____
☐ Business Target Business Name _____
☐ Telephone# Target Home # _____ Cell # _____ Other _____
☐ License Plate Number Target License Plate # _____ ST _____
☐ Address Target Street _____ Apt/FL _____
City _____ State _____ Zip Code _____

EVENT Details

NOTE: All Events are Active until END DATE Specified--- Events are for SHORT TERM LOCATION ENTRIES (Maximum 6 months)

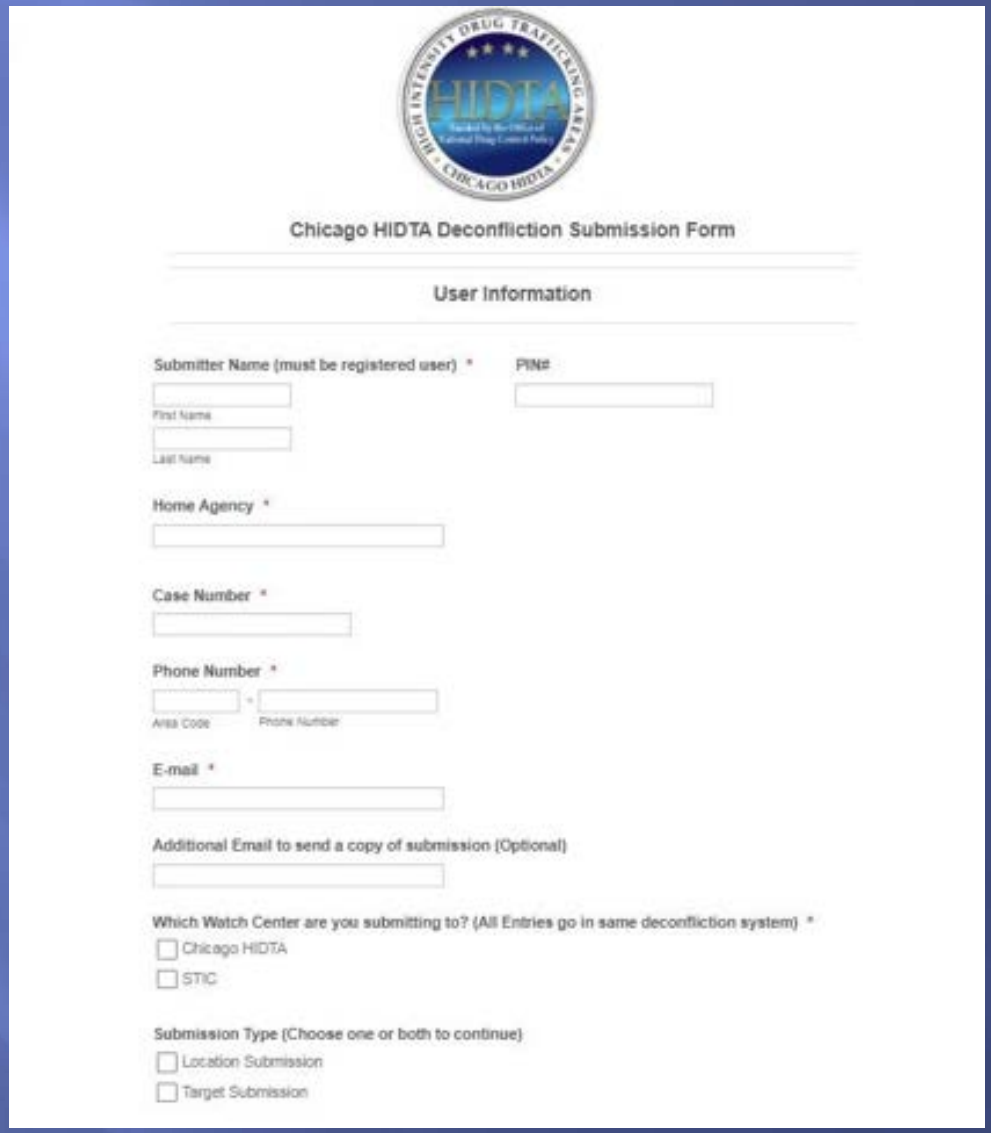
Street _____ City _____
State _____ Zip Code _____ Event Activity* _____
* Designate Event Activity: search/arrest warrant, undercover buy, CI buy, buy/bust, surveillance, reverse
Event Ending Date: *Event will not be submitted without an End Date* _____
Additional Information _____

WatchCenter USE ONLY					Person Making Notification	
Decon Number	DATE	TIME	PERSON NOTIFIED OR	VOICE MESSAGE LEFT	Name	Star#
				Y N		
				Y N		
				Y N		
				Y N		
				Y N		
				Y N		
				Y N		
				Y N		

Use backside of form for additional contact information and Notes

For Official Use Only Revised: December 2012

http://directives.chicagopolice.org/forms/HIDTA_Form.pdf



Chicago HIDTA Deconfliction Submission Form

User Information

Submitter Name (must be registered user) *

First Name

Last Name

PIN#

Home Agency *

Case Number *

Phone Number *

Area Code

Phone Number

E-mail *

Additional Email to send a copy of submission (Optional)

Which Watch Center are you submitting to? (All Entries go in same deconfliction system) *

- Chicago HIDTA
- STIC

Submission Type (Choose one or both to continue)

- Location Submission
- Target Submission

https://www.chicago-hidta.org/submission-form


Target Submission
Target Details
Will be submitted for 2 Years
Subject Name
First Name
Maternal Surname
Last Name
Alias
Alias
Race
Race
Sex
Sex
DOB
Month
Day
Year
IL SID#
FBI#
SSN
DLN
DL State
Other Target Types
Will Be Submitted for 2 Years
Phone Number
Area Code
Phone Number
License Plate#
Include State
Business Name
Online Identifier
Email, Twitter Handle, Etc.
Activity type *
Confirm