CPD Departmental Policy and Constitutional Protections - Legal

S.O. 19-01

This is a summary; For Full Details refer to Order number listed above

Bureau of Detectives SOMEX

POLICY

- **Social media provides an effective means of assisting the Department and its personnel in meeting community outreach, problem solving, investigative, crime prevention, and related objectives**
- **Any social media participation made pursuant to a Department member's official duties is not considered protected speech under the First Amendment**
- **On-Duty Department members will only utilize social media, access social media websites, online aliases, and social media tools for a valid law enforcement purpose**
- **Department members must ensure that all online investigative activities are focused in scope, time and manner to achieve an underlying purpose**

S.O. 19-01

This is a summary; For Full Details refer to Order number listed above

Bureau of Detectives SOMEX

RESPONSIBILITIES

- **Utilize social media to seek and retain information that is:**
  - **Based on criminal predicate or threat to public safety**
  - **Based on reasonable suspicion that an identifiable individual who has committed an identifiable crime or is planning criminal activity**
  - **Relevant to an on-going investigation and prosecution of suspected criminal incidents; the resulting justice system response; or the prevention of crime**
  - **Useful in crime analysis or Officer Safety Bulletins or Informational Bulletins**

S.O. 19-01

This is a summary; For Full Details refer to Order number listed above

Bureau of Detectives SOMEX

RESPONSIBILITIES

- **Do's**
  - **Conduct open source investigative activity**
  - **Collaborate with CCSAO**
  - **Research new social media**
  - **Preserve, prepare and execute search warrants, serve legal process**
  - **Identify potential witnesses and suspects utilizing social media**
- **Do not's**
  - **Retain information on individuals or organizations based on religion, political view, social view or activities**
  - **Retain information on race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless it is relevant to case**
  - **Retain information on age unless is relevant to case**

S.O. 19-01

This is a summary; For Full Details refer to Order number listed above

Bureau of Detectives SOMEX

ASSISTANCE FROM SOMEX

- **To request SOMEX assistance**
  - **Complete Social Media Request [CPD 23.171] form**
  - **Supervisor approval**
  - **Deliver to SOMEX team**

S.O. 19-01

This is a summary; For Full Details refer to Order number listed above

Bureau of Detectives SOMEX

REPORTING AND FILE RETENTION

- **Document all positive investigative results via SOMEX team intelligence report [CPD-23.270]**
  - **Any data of evidentiary value captured on a covert device shall be transferred via CD, DVD or Blue Ray Disk and inventoried along with SOMEX team intelligence report**
- **If a victim or witness consents to allow full access to social media account a Consent to Assume Online Identity Authorization Form [CPD23.271] will be completed and inventoried**
- **Adhere to Department policies regarding technology and records management**
  - **Inquiry Requests Worksheet [CPD-11.704]**
  - **Access to Computerized Data, Dissemination and retention of computer data G.O. 09-01-01**
  - **Local Records Act (50 ILCS 205/1)**
  - **Illinois Freedom of Information Act (5 ILCS 140/1)**
  - **Department records retention schedules**

S.O. 19-01

This is a summary; For Full Details refer to Order number listed above

Bureau of Detectives SOMEX

COVERT ALIAS

- Undercover online activity occurs when SOMEX team member, using online alias, “friends, follows, likes” a person or group for the purpose of building account bona fides
- Social Media Covert Identity Authorization Form [CPD-41.307]
  - Upon approval by Commander, SOMEX team member will notify sergeant who will register the alias with a covert departmental identification number
  - Complete a de confliction
  - Create a unique profile picture that is not attributed to an actual individual
  - Supervisor ensures all forms are completed and covert alias file is maintained and secured in SOMEX office
- Online undercover activity
  - Request verbal authorization to engage in online undercover activity to their exempt supervisor

S.O. 19-01

This is a summary; For Full Details refer to Order number listed above

Bureau of Detectives SOMEX

ONLINE UNDERCOVER INTERACTION

- **Interaction occurs when SOMEX team member, utilizing the online alias, directly interacts with a person online via social media; only when there is reasonable articulable suspicion to believe that criminal offense have been, will be, or are being committed**
- **Online aliases may:**
  - **Request authorization to engage by submitting a To/From subject report to exempt supervisor including**
    - **Online Alias**
    - **Specified unlawful activity**
    - **Social Media accounts utilized**
    - **Valid Law enforcement purpose**
    - **Anticipated duration for the online undercover activity**

S.O. 19-01

This is a summary; For Full Details refer to Order number listed above

Bureau of Detectives SOMEX

IN PERSON UNDERCOVER INTERACTION

- **Interaction occurs when SOMEX team member, utilizing the online alias, directly interacts with a person online via social media; only when there is reasonable articulable suspicion to believe that criminal offense have been, will be, or are being committed**
- **Online aliases may:**
  - **Request authorization to engage by submitting a To/From subject report to exempt supervisor including**
    - **Online Alias**
    - **Specified unlawful activity**
    - **Social Media accounts utilized**
    - **Valid Law enforcement purpose**
    - **Anticipated duration for the online undercover activity**
    - **Operations plan for in person undercover activity**

S.O. 19-01

This is a summary; For Full Details refer to Order number listed above

Bureau of Detectives SOMEX

EQUIPMENT

- **Only approved equipment may be utilized**
- **Ensure equipment is secured at all times**
- **Use non attributable devices**
- **Non attributable devices shall be used for covert activity and never used to access private or personal websites and email in true name or for Department use**

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

Policy

- Information gathered by Department members will be obtained by lawful means in a manner consistent with Department policies, practices and procedures.
- Entry of data into the Department's computerized information systems is restricted to authorized Department members.
- Access to various classifications of information stored on the Department's computerized information systems will be restricted to those Department members authorized by Public Safety Information Technology (PSIT).
- Information contained within the Department's computerized information systems will be disseminated in accordance with Department policy and in compliance with all federal, state and local laws.
- Department members will not purge any information stored in the Department's computerized information systems, unless explicitly authorized.
- Incidental sharing of information from the Department's computerized information systems or remote access by an outside law enforcement agency will conform to the policies and procedures outlined in this directive and will comply with 28 CFR 23

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

Collection and Entry of Information

- Department members will collect information in a lawful manner and in compliance with Department directives and applicable federal, state and local laws.
- Prior to submission for entry into the Department's computerized information systems, Department members making a submission will verify the information contained in the entry.
- Members assigned to enter data will be responsible for accurately entering the data according to the prescribed guidelines.
- Data entered into the Department's computer information systems is subject to the same level of supervisory review as is currently in place for reports submitted on formsets. Information will be attributed to the submitting officer(s).
- Department members will not retain information about any individual or organization gathered solely on the basis of religious, political, or social views or activities; participation in a particular noncriminal organization or lawful event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation. The investigation and related documentation must comply with the Department directives entitled "The First Amendment and Police Actions" and "Information Report System" and all associated addenda.
- NOTE: This prohibition does not apply when the individual or entity is not the subject of an investigation and the reference is Non-criminal Identifying Information tied to an existing criminal report or subject record. Retrieval and use of such information, especially when taken out of context, will be clearly labeled as Non-criminal Identifying Information.

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

Collection and Entry of Information

- Whenever a member assigned/detailed to the Bureau of Detectives or the Bureau of Organized Crime identifies an individual as an active criminal and seeks to enter such information into a criminal intelligence database, the member will:
  - verify that the individual has been assigned an IR, SID and/or FBI number.
  - prepare a Suspect Person/Suspect Vehicle card (CPD-11.460).
  - ensure that the data is current and accurate.
  - forward completed Suspect Person/Suspect Vehicle cards to the division chief.
- The Chief, Bureau of Detectives and the Chief, Organized Crime will:
  - review submitted Suspect Person/Suspect Vehicle cards for conformance to required criteria.
  - ensure only those submissions meeting the established criteria are forwarded to be entered into the Department's computerized information systems.
    - After entry into the Department's computerized information systems, the Suspect Person/Suspect Vehicle card will be returned to the originating unit.
    - Unit files will be maintained in accordance with the forms retention schedule.
  - conduct periodic audits with unit commanders, as outlined in Item IX entitled "Retention."
  - authorize the purging of records as appropriate.

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

Storage and Security

- Public Safety Information Technology (PSIT) is charged with the responsibility of computerized information systems storage and security issues as delineated in the Department directive entitled "Computerized Information Systems."
- Department members have no expectation of privacy in the use of Department computers or related equipment. Individuals may be subject to monitoring while using any of the Department's computers or accessing the computerized information systems.
- Each Department member will be issued a Logon ID and will be responsible for its security and accountable for its use. Members will not use another member's logon ID under any circumstances. All access including, but not limited to, Local Area Networks (LANs), Wide Area Networks (WANs), information system interfaces, entry terminals and administration terminals requires an authorized log-on and password.
- Department computerized information systems are designed with transaction logs for the purpose of establishing audit trails and back-up sets.
- Periodic audits for 28 CFR 23 compliance will be conducted to monitor Criminal Intelligence Information access and usage.
  - PSIT will establish procedures to conduct audits of electronic submissions.
  - The Inspection Division will establish procedures to conduct periodic audits of "Inquiry Request Worksheets" (CPD-11.704).

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

Access to Computerized Information

- **Access to information or files maintained in the Department's computerized information system is granted only when authorized and by means of the log-on process on Department owned/leased equipment through authorized networking protocols and procedures.**

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

Dissemination of Information

- **Records, files or reports may be printed from computerized information systems and/or duplicated by Department personnel for Department use only, except as provided in this section.**
  - **Public Release**
  - **Incidental Sharing of Information with Outside Agencies**

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

- The Department recognizes that some criminal activity may affect multiple jurisdictions. Whenever possible, the Department will provide outside law enforcement agencies engaged in an active investigation access to information which is relevant to that investigation.
- Department members receiving a request for information from an outside agency, whether in person, by phone or by fax, will:

  - verify the identity and agency of the requester prior to making a query
  - submit a query if satisfied that the prerequisites in Item VII-C-1-a of the diretive have been met. If a query is made on behalf of an outside agency and the Department's computerized information system returns:

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

- Data which is classified as "Criminal Intelligence Information," the member will have a sworn supervisor approve the "Inquiry Request Worksheet" (CPD-11.704) prior to disseminating the information.
- Data which is labeled as "Non-criminal Identifying Information," the member will determine if the information is relevant to the requester's needs.
  - If the "Non-criminal Identifying Information" is not relevant to the inquiring agency's needs, the member will not divulge this information.
  - If the "Non-criminal Identifying Information" is relevant to the investigation, the member will have a sworn supervisor approve the "Inquiry Request Worksheet" prior to disseminating the information.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

- Data which is not labeled as "Criminal Intelligence Information" or "Noncriminal Identifying Information," the member will make a determination:
  - If the information serves a legitimate law enforcement purpose, it may be disseminated.
  - If the information does not serve a legitimate lawful purpose, it will not be disseminated.
- Sworn supervisors reviewing an "Inquiry Request Worksheet" will:
  - determine if the "Need to Know/Right to Know" criteria has/have been satisfied.
  - ensure that a 28 CFR 23 notification is printed upon the hard copy report delivered to the agency representative.
  - ensure the agency representative has signed the "Inquiry Request Worksheet." A signed facsimile copy will suffice for phone inquiries.
  - forward the completed "Inquiry Request Worksheet" to PSIT.
- PSIT will forward one copy of the completed "Inquiry Request Worksheet" to the owner of the data

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

Self Contained Information Systems

- **Any unit that maintains investigative records or criminal intelligence information on a system that is self-contained is expressly prohibited from sharing any information contained on that system with any outside agency**

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

Retention

- **Information in the Department's computerized information systems will adhere to the Department's Form Retention Schedule and all applicable federal, state and local laws.**
- **Department members will not remove or alter any official record, file or report from the Department's computerized information systems, unless explicitly authorized.**
- **PSIT will preserve transaction logs in a manner consistent with operational functionality and in accordance with the Department's retention schedule and in compliance with all federal, state and local laws.**

G.O. G09-01-01

This is a summary; For Full Details refer to Order number listed above

Access to Computerized Data, Dissemination and Retention of Computer Data

Retention

- **The Owner of the Data labeled as Criminal Intelligence Information or Non-criminal Identifying Information will be responsible for reviewing on a periodic basis the validity of such information.**
  - **Inaccurate or outdated information should be deleted.**
  - **Whenever a member assigned/detailed to the Bureau of Detectives or the Bureau of Organized Crime determines that a suspect person or vehicle record is no longer appropriate the member will remove the Suspect Person/Suspect Vehicle card from the unit file, check the "Delete" box and enter his star number in the "Remarks" section of the card. The card will be submitted through the chain of command to the division chief for authorization of the records purge.**
  - **Additions to a record will be dated.**
  - **Modifications to a record which correct errors or negate an individual's classification as a suspect must be reported to any agency that received such erroneous information.**
  - **Owners of data will submit an annual report, through their respective chain of command, to the Chief, Bureau of Administration certifying that the records in the Department's computerized information systems have been verified.**
- **PSIT will purge Criminal Intelligence records no later than five years from the last validated entry.**

G.O. G09-01-03

This is a summary; For Full Details refer to Order number listed above

Use of Internet

Policy

- **It is the Department's policy to use the Internet and the Department's home page on the World Wide Web to disseminate information, such as official Department reports, press releases, information, and other data routinely released to the public and to provide appropriate services that encourage police-community partnerships and enhance cooperative problem solving.**

G.O. G09-01-03

This is a summary; For Full Details refer to Order number listed above

Use of Internet

- Members using Department resources to access the Internet will be restricted to official Department business.
- Members will not download any material for personal use or software of any kind without the prior approval from the Director, ISD.
- Information will not be disseminated through the Internet by Department members as delineated in the Department directive titled "Department Reports, Publications, Survey Responses, and Official Statistics."
- Department-owned commercial or developed software for the Internet will not be used for personal use.
- Links contained within Department home pages are limited to Department-approved agencies.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-03

This is a summary; For Full Details refer to Order number listed above

Use of Internet

All authorized users of City and Department Internet and e-mail must:

- check their Department email at least once per tour of duty;
- adhere to the provisions of all existing Department rules and directives, specifically the:
  - Department's Internet and E-Mail Use Policy, and
  - Department directive titled "Department–Issued Electronic Communication Devices;"
- promptly report any breaches of computer security to the Information Services Help Desk at 4-DATA;
- be in compliance with all federal and state laws;
- conform to all City of Chicago ordinances and Department policies and procedures;
- strive to minimize undue strain on the City's and Department's computer networks and disruption to others;
- not disclose the contents or existence of City or Department computer files, e-mail, or other information to anyone other than authorized recipients.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-03

This is a summary; For Full Details refer to Order number listed above

Use of Internet

- City and Department Internet and e-mail resources are to be used for Department business only.
- Department members who receive an e-mail of a criminal nature requiring immediate action (threats, reports of abuse, harassment, etc.) will immediately notify their sworn supervisor. The notified sworn supervisor will:

  - determine if the completion of a case report is necessary to document the incident.

  - ensure a preliminary investigation is completed and the proper notifications are made.
- The City of Chicago and the Chicago Police Department have the right to monitor Internet and e-mail use to ensure that these resources are being used for Departmental business purposes only.
- No outgoing messages on City or Department Internet or e-mail may purport to make a statement of City or Department policy, either expressly or by implication, except for messages that quote ordinances or other sources of City and/or Department policy, or messages approved by the Superintendent of Police.

This is a summary; For Full Details refer to Order number listed on slide

G09-01-05

This is a summary; For Full Details refer to Order number listed above

Department-Issued Electronic Communications Devices

- For the purposes of this directive, Department-issued electronic communication devices will be considered any device, issued by the Department, which gives members the ability to communicate via voice, internet, Email, instant messages, text messages, or multimedia messages over a cellular or wireless telecommunications network.
- Department-issued electronic communication devices (e.g., BlackBerry devices) are issued to members as a convenience to enhance on-duty job performance only.
- Department members: 1. are not obligated or required to access, respond to electronic communications, and/or carry the devices on their person while off-duty. 2. have no expectation of privacy regarding any communication made with or the files stored on Department-issued devices. Administrative searches of electronic files may be conducted as deemed necessary by Department supervisory or command personnel without prior notice to the affected member and without the existence of probable cause or the procurement of a search warrant.
- Off-duty members will not use a Department-issued electronic communication device to access their Department e-mail account, respond to electronic messages, or perform other work related to Department business unless the member is officially on a "call-back" assignment as defined by existing labor contractual agreements or the member is directed by a supervisor to immediately perform any work and overtime is authorized by the supervisor directing the request. If there is a request and approval for overtime, the Department member must comply with the applicable Department directives concerning the submission of an Overtime/Compensatory Time Report (CPD-11.608). If overtime is not approved, the member is not to perform the work. NOTE: This guideline includes accessing electronic messages using personally owned electronic communication devices.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-05

This is a summary; For Full Details refer to Order number listed above

Department-Issued Electronic Communications Devices

Members issued a Department-issued electronic communication device will:

- **read, complete, and obtain the proper signatures as indicated on the Department-Issued Electronic Communication Device Compliance Statement (CPD-65.109) and E-Mail Compliance Statement form (CPD-65.118).**
- **adhere to the provisions of existing Department rules and existing directives, specifically the Department's Internet and E-Mail Use Policy and Department directive entitled "Use of the Internet."**
- **limit personal use to emergency, incidental, and/or reasonably necessary calls.**
- **NOT take pictures/video with the device unless as a part of official business.**

  NOTE: Pictures and videos taken with a Department-issued electronic communication device that has evidentiary value will be inventoried in accordance with the Department directives entitled "Inventory System for Property Taken Into Custody."
- **NOT access and/or post information to social networking websites unless as a part of official business.**
- **NOT install or use any unauthorized software or applications on the device.**

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-05

This is a summary; For Full Details refer to Order number listed above

Department-Issued Electronic Communications Devices

Supervisory personnel will:

- ensure that their subordinates use Department-issued electronic communication devices as prescribed.
- take immediate corrective and/or disciplinary action if a member is observed or reported to be improperly handling, operating, or in any way damaging a Department-issued electronic communication device.
- conduct an investigation when a Department-issued electronic communication device is:

  - damaged, and: (1) ensure that appropriate reports are prepared. (2) obtain a Complaint Register (CR) number if the damage was caused by a member's neglect or willful conduct. (3) submit a To-From-Subject report detailing the nature and cause of the damage and the CR number, if applicable, through channels, to the Managing Deputy Director, Public Safety Information Technology (PSIT).
  - lost or stolen, and: (1) ensure that the appropriate case report is prepared and, if appropriate, obtain a CR number. Copies of all reports will be sent through channels to the Managing Deputy Director, PSIT. (2) ensure that a facsimile message is sent to all districts.

- Members not assigned to the Bureau of Organized Crime will report equipment malfunctions to the Help Desk.
- An exempt member or unit commanding officer may authorize the administrative search of a Department-issued electronic device.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-06

This is a summary; For Full Details refer to Order number listed above

Use of Social Media Outlets

- Social media outlets, when used in a proper manner, can reinforce the Department's relationship with the public, build community support, and assist in solving crime. Department members have a constitutional right to express their views under the First Amendment. However, Department members may be subject to discipline for violating the provisions of this directive. Any social media participation made pursuant to a Department member's official duties is not considered protected speech under the First Amendment.
- For the purposes of the directive, the term "social media outlets" means any electronic communication (such as personal Web sites, outlets for social networking, and microblogging) through which participants utilize online communities to share information, ideas, personal messages, and other content through an electronic format. These formats include, but are not limited to, text, video, photographs, audio, digital documents, etc.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-06

This is a summary; For Full Details refer to Order number listed above

Use of Social Media Outlets

When using social media, whether on or off duty, Department members are prohibited from posting, displaying, transmitting, or otherwise disseminating:

1. anv communications that discredit or reflect poorly on the Department, its vision, mission, values, or goals.
2. confidential information related to Department training, activities, or on-going investigations without express written permission.
3. content that is disparaging to a person or group based on race, color, sex, gender identity, age, religion, disability, national origin, ancestry, sexual orientation, marital status, parental status, military status, source of income, credit history, criminal record, criminal history, or any other protected class consistent with the Department directives titled "Human Rights and Human Resources" and "Prohibition Regarding Racial Profiling and Other BiasBased Policing."

- The policies outlined in the directive address the full breadth and scope of social media rather than any one particular format. The Department recognizes that as technology advances, new methods for social media participation will emerge.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-06

This is a summary; For Full Details refer to Order number listed above

Use of Social Media Outlets

- When using social media, whether on or off duty, Department members should be mindful that their communications become part of the worldwide electronic public domain. Department members should be aware that privacy settings and social media sites are subject to constant modifications, and they should never assume that personal information posted on such sites is protected or secure.
- Department members should expect that any information that they create, transmit, download, exchange, or discuss that is available online in a public forum may be accessed by the Department without prior notice.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-06

This is a summary; For Full Details refer to Order number listed above

Use of Social Media Accounts- Department-Authorized Social Media Accounts

- All Department social media outlets will be approved by the Superintendent or a designee.
- The use of Department computers and Department-issued electronic communication devices by Department members to access any social media outlet is prohibited absent prior supervisory approval. Supervisory approval will be on an individual basis or based on a specific job assignment or responsibility.
- Social media content will adhere to applicable laws, the Rules and Regulations of the Chicago Police Department, and any relevant Department policies, including all information-technology and records-management policies.
- Access to Department social media accounts and the internet will be consistent with the Department directives titled "Use of the Internet," "Department-Issued Electronic Communication Devices," and "Social Media Outlet: Twitter."
- Department records-retention schedules will apply to social media content and is subject to the Local Records Act (50 ILCS 205/1), consistent with the Department directive titled "Records Management."
- Content will be managed, stored, and retrievable in compliance with the Illinois Freedom of Information Act (5 ILCS 140/1) and consistent with the Department directive titled "Freedom of Information."

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-06

This is a summary; For Full Details refer to Order number listed above

Use of Social Media Accounts- Department-Authorized Social Media Accounts

Department members authorized to administer Department social media outlets will:

- conduct themselves at all times as representatives of the Department and, accordingly, adhere to applicable Department Rules and Regulations and Department directives.
- not make statements indicating the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions.
- comply with all copyright, trademark, and service-mark restrictions in posting materials to electronic media. d. ensure that all relevant privacy protections are maintained.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-06

This is a summary; For Full Details refer to Order number listed above

Use of Social Media Outlets- Department Member's Personal Social Media Accounts

In addition to the prohibitions outlined in the directive, when using their personal social media accounts, Department members are prohibited from posting, displaying, transmitting, or otherwise disseminating:

- Department information, records, documents, video recordings, audio recordings, or photographs to which they have access as a result of their employment without the written permission from the Communications Division or the Superintendent or a designee.
- any references to any other Department member's employment by the Department without that person's consent.
- any intellectual property of the Department or the City of Chicago without the specific authorization of the Superintendent or a designee. Department or City of Chicago intellectual property includes but is not limited to logos, uniforms, official photographs, audio/ video files, or any text documents (paper or electronic)
- any information representing themselves as an official spokesperson of the Department and the City of Chicago unless specifically authorized by the Superintendent or a designee.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-06

This is a summary; For Full Details refer to Order number listed above

Use of Social Media Outlets- Use of Social Media Outlets for Investigative Purposes

Social media is a valuable investigative tool when seeking evidence or information about:

- missing persons;
- wanted persons;
- gang violence and retaliation;
- crimes perpetrated online (e.g., cyberbullying, cyberstalking);
- photos or videos of a crime posted by a participant or observer;
- criminal participation and retaliation;
- acquiring information or intelligence that may be useful for criminal investigations or allocating resources for public safety;
- aiding the coordination and deployment of police resources; and
- administrative and criminal investigations by the Bureau of Internal Affairs.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-06

This is a summary; For Full Details refer to Order number listed above

Use of Social Media Outlets- Use of Social Media Outlets for Investigative Purposes

- Exempt commanding officers of units that conduct investigations using social media will establish standard operating procedures and unit-level protocols created in consultation with the Legal Affairs Section and the Information Services Division.

Department members utilizing a social media outlet as an investigative tool will:

- use only Department-approved electronic equipment throughout the investigation;
- conduct an investigation only while on duty;
- follow the guidelines set forth in the Rules and Regulations of the Chicago Police Department and the the investigative and reporting guidelines outlined in the appropriate Department directives including, but not limited to: "The First Amendment and Police Actions," "Investigations Directed at First Amendment-Related Information," "Other Police Action Which May Impact First Amendment Conduct."
- barring a warrant, exigent circumstances, or prior authorization under the provisions of the directive, only use publicly available material or information that is posted in a publicly accessible format;
- forward any credible leads to the appropriate investigative unit;
- notify the Communications Division of social media posts that will likely generate media inquiries or interest; and
- document the use of social media as an investigative tool in the appropriate reports.

This is a summary; For Full Details refer to Order number listed on slide

G.O. G09-01-06

This is a summary; For Full Details refer to Order number listed above

Use of Social Media Outlets- Use of Social Media Outlets for Investigative Purposes

Department members utilizing a social media outlet as an investigative tool will NOT:

- monitor a suspect solely based on his or her non-criminal political beliefs or expressions.
- use their personal social media account or personal account information to access the social media content.
- use another individual's personal account without his or her consent and the approval of the appropriate bureau chief.

This is a summary; For Full Details refer to Order number listed on slide

S.O. S02-03-010

This is a summary; For Full Details refer to Order number listed above

Social Media Outlet: Twitter

- Twitter is an online social networking and microblogging service that enables its users to send and read text-based messages known as "tweets."
- Twitter is a means to connect the Department to the community in real time. The Department uses Twitter as a tool to inform and build relationships with community members.
- The Chicago Police Department is committed to serving the community and recognizes that current technology, when utilized properly, can provide the Department and community with an essential channel of communication.
- Each district will have a Twitter presence and will disseminate the following types of information: vetted crime prevention tips, success stories, community events, and other district-specific events.

This is a summary; For Full Details refer to Order number listed on slide

28 CFR PART 23

This is a summary; For Full Details refer to Order number listed above
Source: ecfr.gov-electronic code of federal regulations

Criminal Intelligence Operating Policy

- The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq.,*

28 CFR PART 23

This is a summary; For Full Details refer to Order number listed above
Source: ecfr.gov-electronic code of federal regulations

Criminal Intelligence Operating Policy

- It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.
- These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq.*,

28 CFR PART 23

This is a summary; For Full Details refer to Order number listed above
Source: ecfr.gov-electronic code of federal regulations

Criminal Intelligence Operating Policy

- A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.
- 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.
- *Reasonable Suspicion* or *Criminal Predicate* is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

28 CFR PART 23

This is a summary; For Full Details refer to Order number listed above
Source: ecfr.gov-electronic code of federal regulations

Criminal Intelligence Operating Policy

- A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.
- A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.
- project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage.
- All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance.

28 CFR PART 23

This is a summary; For Full Details refer to Order number listed above
Source: ecfr.gov-electronic code of federal regulations

Criminal Intelligence Operating Policy

- If funds awarded under the Act are used to support the operation of an intelligence system, then: (1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and (2) A project shall undertake no major modifications to system design without prior grantor agency approval.
- A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.
- A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

28 CFR PART 23

This is a summary; For Full Details refer to Order number listed above
Source: ecfr.gov-electronic code of federal regulations

Criminal Intelligence Operating Policy

- A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.
- A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.
- A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives.
- he Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

1ST AMENDMENT

SOURCE: LAW.CORNELL.EDU

- Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.
- The First Amendment guarantees freedoms concerning religion, expression, assembly, and the right to petition. It forbids Congress from both promoting one religion over others and also restricting an individual's religious practices. It guarantees freedom of expression by prohibiting Congress from restricting the press or the rights of individuals to speak freely. It also guarantees the right of citizens to assemble peaceably and to petition their government.

1st Amendment- G.O. 02-02

First Amendment conduct means speech or activity related to the freedom of speech, free exercise of religion, freedom of the press, the right to assemble, and the right to petition the government. The First Amendment protects, but is not limited to, the following rights:

- The right to hold ideas or beliefs concerning public or social policy, or political, educational, cultural, economic, philosophical or religious matters;
- The right to communicate or receive such ideas or beliefs, publicly or privately, orally, in writing or by symbolic means;
- The right to associate and assemble publicly or privately with other persons concerning ideas or beliefs about public or social policy, or political, educational, cultural, economic, philosophical or religious matters (but not a right to associate or assemble for purposes unrelated to the right to hold and express such ideas or beliefs);

This is a summary; For Full Details refer to Order number listed on slide

1st Amendment- G.O. 02-02

- The right to advocate ideas or beliefs, including the right to advocate an alternative system of government and to advocate "the use of force or of law violation, except where such advocacy is directed to inciting or producing imminent lawless conduct and is likely to incite or produce such action“
- The right to petition the government or governmental officials for redress of grievances;
- The right to associate for the purpose of seeking and giving legal advice as well as advancing litigation.

First Amendment rights exercised in public forums may be subject to content-neutral time, place, and manner regulations that support an appropriate governmental interest.

This is a summary; For Full Details refer to Order number listed on slide

4TH AMENDEMNT

SOURCE: LAW.CORNELL.EDU

- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
- The Fourth Amendment originally enforced the notion that "each man's home is his castle", secure from unreasonable searches and seizures of property by the government. It protects against arbitrary arrests, and is the basis of the law regarding search warrants, stop-and-frisk, safety inspections, wiretaps, and other forms of surveillance, as well as being central to many other criminal law topics and to privacy law.

4th Amendment- G.O. 02-02

- "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."
- What a person seeks to preserve as private, including oral communications, even in an area accessible to the public, may be constitutionally protected under the Fourth Amendment.
- The Fourth Amendment protects against governmental intrusion not justified by an appropriate governmental interest.

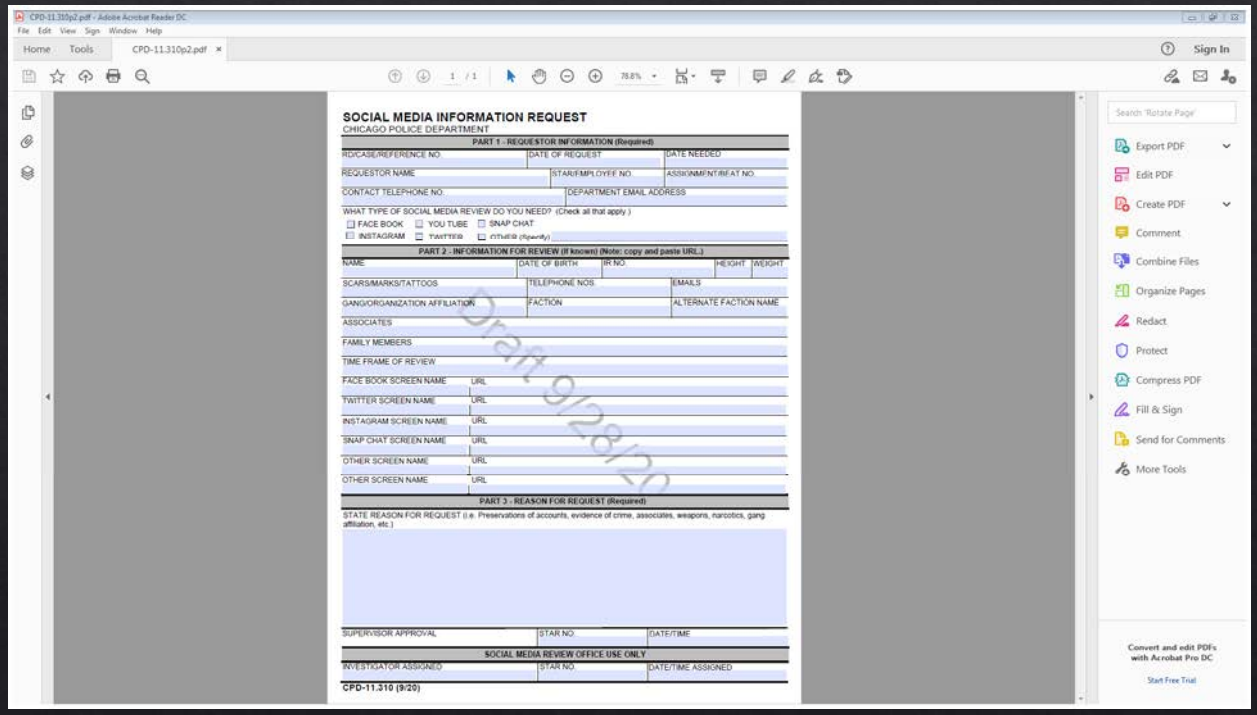
This is a summary; For Full Details refer to Order number listed on slide

14TH ADMENDEMENT

SOURCE: SOURCE: LAW.CORNELL.EDU

- All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.
- The Fourteenth Amendment addresses many aspects of citizenship and the rights of citizens. The most commonly used -- and frequently litigated -- phrase in the amendment is "equal protection of the laws", which figures prominently in a wide variety of landmark cases, including Brown v. Board of Education (racial discrimination), Roe v. Wade (reproductive rights), Bush v. Gore (election recounts), Reed v. Reed (gender discrimination), and University of California v. Bakke (racial quotas in education).

Social Media Information Request Form



SOCIAL MEDIA INFORMATION REQUEST
CHICAGO POLICE DEPARTMENT

PART 1 - REQUESTOR INFORMATION (Required)

RD/CASE/REFERENCE NO. | DATE OF REQUEST | DATE NEEDED
REQUESTOR NAME | STAR/EMPLOYEE NO. | ASSIGNMENT/BEAT NO.
CONTACT TELEPHONE NO. | DEPARTMENT EMAIL ADDRESS

WHAT TYPE OF SOCIAL MEDIA REVIEW DO YOU NEED? (Check all that apply.)
☐ FACE BOOK ☐ YOU TUBE ☐ SNAP CHAT
☐ INSTAGRAM ☐ TWITTER ☐ OTHER (Specify)

PART 2 - INFORMATION FOR REVIEW (If known) (Note: copy and paste URL.)

NAME | DATE OF BIRTH | IR NO. | HEIGHT | WEIGHT
SCARS/MARKS/TATTOOS | TELEPHONE NOS. | EMAILS
GANG/ORGANIZATION AFFILIATION | FACTION | ALTERNATE FACTION NAME
ASSOCIATES
FAMILY MEMBERS
TIME FRAME OF REVIEW
FACE BOOK SCREEN NAME | URL
TWITTER SCREEN NAME | URL
INSTAGRAM SCREEN NAME | URL
SNAP CHAT SCREEN NAME | URL
OTHER SCREEN NAME | URL
OTHER SCREEN NAME | URL

PART 3 - REASON FOR REQUEST (Required)

STATE REASON FOR REQUEST (i.e. Preservations of accounts, evidence of crime, associates, weapons, narcotics, gang affiliation, etc.)

SUPERVISOR APPROVAL | STAR NO. | DATE/TIME

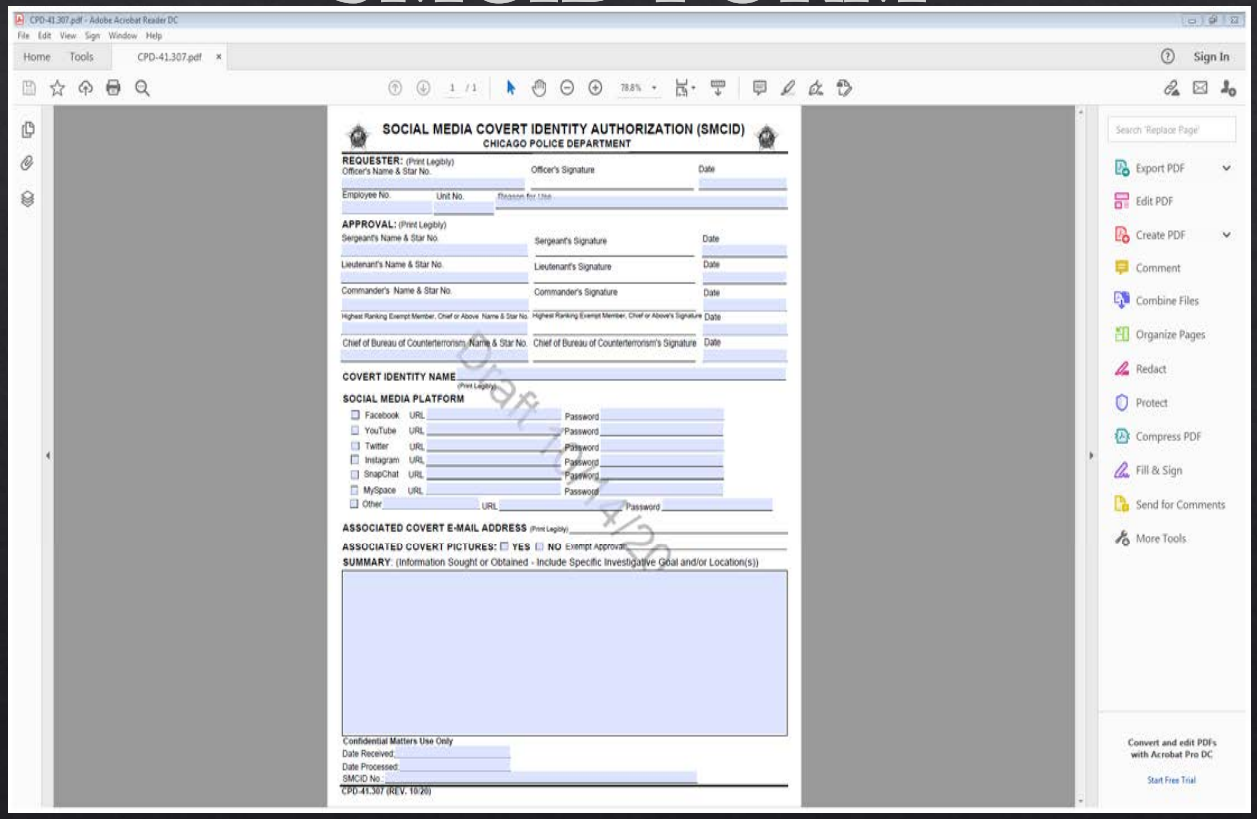
SOCIAL MEDIA REVIEW OFFICE USE ONLY

INVESTIGATOR ASSIGNED | STAR NO. | DATE/TIME ASSIGNED

CPD-11.310 (9/20)

Draft 9/28/20

SMCID FORM



CPD-41.307.pdf - Adobe Acrobat Reader DC

File Edit View Sign Window Help

Home Tools CPD-41.307.pdf

Sign In

SOCIAL MEDIA COVERT IDENTITY AUTHORIZATION (SMCID)
CHICAGO POLICE DEPARTMENT

REQUESTER: (Print Legibly)
Officer's Name & Star No. | Officer's Signature | Date
Employee No. | Unit No. | Reason for Use

APPROVAL: (Print Legibly)
Sergeant's Name & Star No. | Sergeant's Signature | Date
Lieutenant's Name & Star No. | Lieutenant's Signature | Date
Commander's Name & Star No. | Commander's Signature | Date
Highest Ranking Exempt Member, Chief or Above Name & Star No. | Highest Ranking Exempt Member, Chief or Above's Signature | Date
Chief of Bureau of Counterterrorism Name & Star No. | Chief of Bureau of Counterterrorism's Signature | Date

COVERT IDENTITY NAME (Print Legibly)

SOCIAL MEDIA PLATFORM

- ☐ Facebook URL Password
- ☐ YouTube URL Password
- ☐ Twitter URL Password
- ☐ Instagram URL Password
- ☐ SnapChat URL Password
- ☐ MySpace URL Password
- ☐ Other URL Password

ASSOCIATED COVERT E-MAIL ADDRESS (Print Legibly)

ASSOCIATED COVERT PICTURES: ☐ YES ☐ NO Exempt Approval

SUMMARY: (Information Sought or Obtained - Include Specific Investigative Goal and/or Location(s))

Confidential Matters Use Only
Date Received
Date Processed
SMCID No.

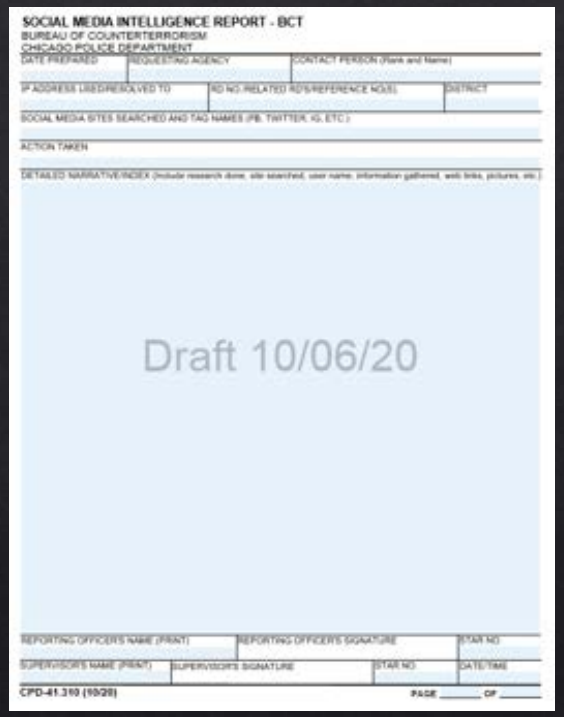
CPD-41.307 (REV. 10/20)

Draft 11/4/20

Export PDF
Edit PDF
Create PDF
Comment
Combine Files
Organize Pages
Redact
Protect
Compress PDF
Fill & Sign
Send for Comments
More Tools

Convert and edit PDFs with Acrobat Pro DC
Start Free Trial

Social Media Intelligence Report-BCT



SOCIAL MEDIA INTELLIGENCE REPORT - BCT

BUREAU OF COUNTERTERRORISM
CHICAGO POLICE DEPARTMENT

DATE PREPARED | REQUESTING AGENCY | CONTACT PERSON (Rank and Name)

IP ADDRESS USED/RESOLVED TO | RD NO./RELATED RD'S/REFERENCE NO(S). | DISTRICT

SOCIAL MEDIA SITES SEARCHED AND TAG NAMES (FB, TWITTER, IG, ETC.)

ACTION TAKEN

DETAILED NARRATIVE/INDEX (Include research done, site searched, user name, information gathered, web links, pictures, etc.)

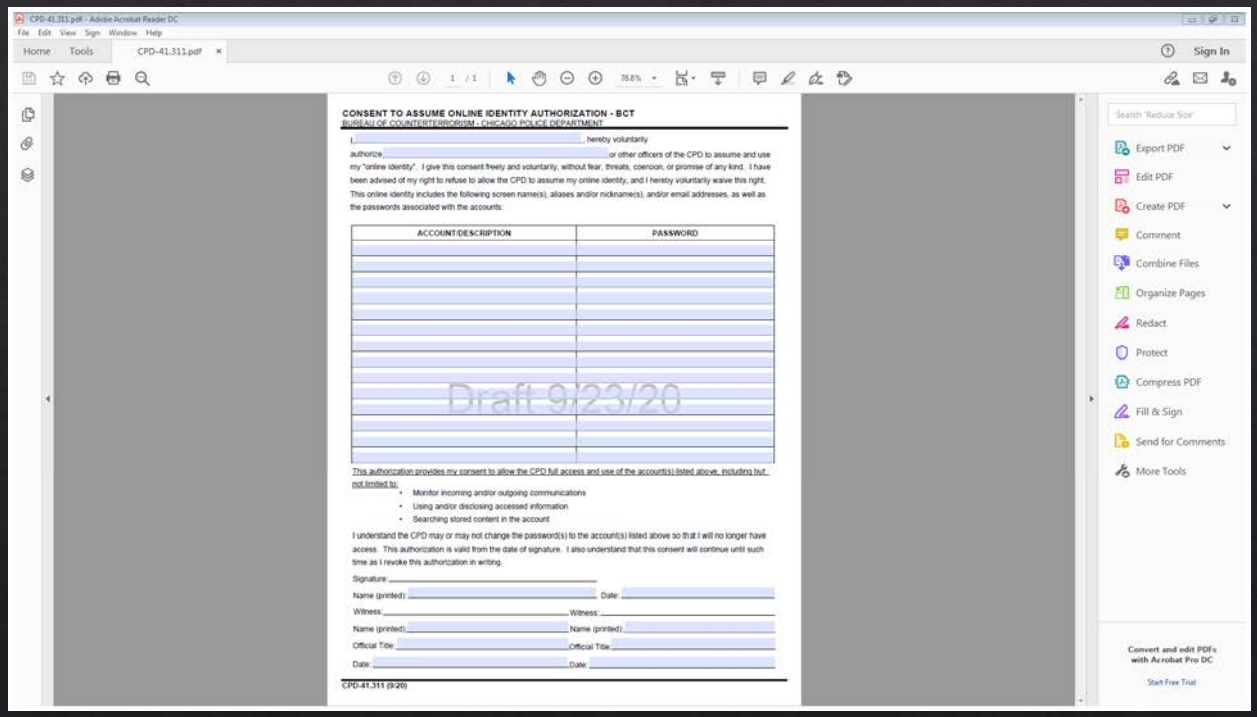
Draft 10/06/20

REPORTING OFFICER'S NAME (PRINT) | REPORTING OFFICER'S SIGNATURE | STAR NO.

SUPERVISOR'S NAME (PRINT) | SUPERVISOR'S SIGNATURE | STAR NO. | DATE/TIME

CPD-41.310 (10/20) PAGE _____ OF _____

Consent to Assume Online ID Authorization



CONSENT TO ASSUME ONLINE IDENTITY AUTHORIZATION - BCT

BUREAU OF COUNTERTERRORISM - CHICAGO POLICE DEPARTMENT

I, _____, hereby voluntarily authorize _____ or other officers of the CPD to assume and use my "online identity". I give this consent freely and voluntarily, without fear, threats, coercion, or promise of any kind. I have been advised of my right to refuse to allow the CPD to assume my online identity, and I hereby voluntarily waive this right. This online identity includes the following screen name(s), aliases and/or nickname(s), and/or email addresses, as well as the passwords associated with the accounts:

ACCOUNT/DESCRIPTION	PASSWORD

Draft 9.23/20

This authorization provides my consent to allow the CPD full access and use of the account(s) listed above, including but not limited to:

- Monitor incoming and/or outgoing communications
- Using and/or disclosing accessed information
- Searching stored content in the account

I understand the CPD may or may not change the password(s) to the account(s) listed above so that I will no longer have access. This authorization is valid from the date of signature. I also understand that this consent will continue until such time as I revoke this authorization in writing.

Signature: _____

Name (printed): _____ Date: _____

Witness: _____ Witness: _____

Name (printed): _____ Name (printed): _____

Official Title: _____ Official Title: _____

Date: _____ Date: _____

CPD-41.311 (9/20)

CPD Departmental Policy and Constitutional Protections - Legal

ORDERS COVERED

- G.O. G02-02 **The First Amendment and Police Action**
- G.O. G02-02-01 **Investigations Directed at First Amendment – Related Information**
- S.O. 02-02-01 **Investigations Directed at First Amendment – Related Information**
- B.C.T. S.O. 20-01 **Utilization of Social Media – Bureau of Counterterrorism**
- S.O. 19-01 **Bureau of Detectives SOMEX**
- G.O. G09-01-01 **Access to Computerized Data, Dissemination and Retention of Computer Data**
- G.O. G09-01-03 **Use of Internet**
- G.O. G09-01-05 **Department-Issued Electronic Communications**
- G.O. G09-01-06 **Use of Social Media**
- S.O. S02-03-10 **Social Media Outlet: Twitter**

CPD Departmental Policy and Constitutional Protections - Legal

QUESTIONS?