

# GENERAL ORDER



DISTRICT OF COLUMBIA

|  |
|--|
| <b>Title</b>   |
| <b>Suspicious Activity Reporting Program</b>   |
| <b>Topic / Number</b>  |
| <b>GO-HSC-802.06</b>   |
| <b>Effective Date</b>  |
| <b>August 19, 2011</b>   |
| <b>Replaces:</b><br>GO-HSC-802.06 (Suspicious Activity Reporting Program), Effective Date January 16, 2009   |
| <b>Related to:</b><br>GO-SPT-302.09 (Use and Operation of Mobile Data Computers), Effective Date May 7, 2001<br>GO-SPT-401.01 (Field Reporting System), Effective Date March 4, 2004<br>SO-08-02 (Duties and Responsibilities of Reviewing PD Forms 251, 252, and PD form 10's for Accuracy, Completeness and CCN Reconciliation), Effective Date April 11, 2008 |

|       |  |         |
|-------|--|---------|
| I.    | Background   | Page 1  |
| II.   | Policy   | Page 1  |
| III.  | Definitions  | Page 2  |
| IV.   | Regulations  | Page 5  |
| V.    | Procedures   | Page 6  |
| V.A.  | Suspicious Activity Reports                                | Page 6  |
| V.B.  | Suspicious Activity Report-Related Contacts and Stops      | Page 7  |
| V.C.  | Suspicious Activity Report-Related Offense/Incident Report | Page 8  |
| VI.   | Roles and Responsibilities                                 | Page 8  |
| VII.  | Cross Reference  | Page 10 |
| VIII. | Attachment   | Page 10 |

## I. BACKGROUND

All persons living or working in, or visiting, the United States of America play a critical role in preventing crimes and acts of terrorism. Law enforcement officers must also carry out counter-terrorism responsibilities within the broader context of our core mission of providing effective professional police service in order to prevent and deter crime, violence, and disorder. In order to support Metropolitan Police Department members in preventing criminal conduct and acts of terrorism, the Homeland Security Bureau is initiating the Suspicious Activity Reporting Program.

The purpose of this General Order is to provide guidance for the operation of the Suspicious Activity Reporting Program. The program will provide a mechanism for members to report suspicious activity discovered in the course of routine or specialized patrol and in initial and follow-up investigations. The observations and information reported by members will provide valuable intelligence for detecting and preventing criminal conduct and acts of terrorism.

## II. POLICY

It is the policy of the Metropolitan Police Department to lawfully collect, maintain, and disseminate intelligence information, while safeguarding civil liberties and privacy

protections, in order to protect the public from criminal conduct and acts of terrorism.

### III. DEFINITIONS

- A. When used in this order, the following terms shall have the meaning designated:
1. Involved Party (IP) – Individual who has been observed engaging in suspicious activity, when no definitive criminal activity can be identified, thus precluding his/her identification as a suspect.
  2. iWatchDC – Website used to report suspicious activities or behaviors that may indicate criminal or terrorist activity.
  3. Member – Sworn employee of the MPD or MPD Reserve Corps member.
  4. PD Form 76 (Stop or Contact Report) – MPD form currently used to record non-forcible stops and contacts.
  5. PD Form 251 (Incident-Based Event Report) – MPD form currently used to report forcible stops and frisks, offenses, and incidents.
  6. Personally Identifiable Information (PII) – Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual. This includes, but is not limited to, information which can be used to distinguish or trace an individual's identity (e.g., his/her name, social security number, date and place of birth).
  7. Suspicious Activity – Reported or observed questionable behavior or circumstances, including, but not limited to, the following:
    - a. Person(s) engaged in suspected pre-operational surveillance involving the use of binoculars or cameras, taking measurements, drawing diagrams, etc.;
    - b. Person(s) engaged in counter-surveillance efforts (e.g., doubling back, changing appearance, evasive driving);
    - c. Person(s) engaging in conversation with security personnel focusing on sensitive subjects (e.g., security information, hours of operation, shift changes, what security cameras film);
    - d. Person(s) taking measurements (e.g., by counting footsteps, by measuring building entrances or perimeters, distances between security locations, distances between cameras);

- e. Person(s) taking photographs or video footage with no apparent aesthetic value (e.g., from various camera angles; and of security equipment, security personnel, traffic lights, building entrances);
- f. Person(s) drawing diagrams or taking notes (e.g., is/are interested in building plans, locations of security cameras or security personnel, security shift changes, weak security points);
- g. Person(s) observed abandoning a suspicious package or item (e.g., suitcase, backpack, bag, box, package);
- h. Person(s) observed abandoning a vehicle in a secured or restricted location (e.g., front of a government building, airport, sports arena);
- i. Person(s) attempting to enter secured or sensitive premises or an area without authorization (e.g., area for only "official personnel", closed off areas of an airport, harbor, secured area at a significant event attended by elected officials, diplomats, or other dignitaries);
- j. Person(s) engaged in testing of existing security measures (e.g., by a "dry run", security breach of perimeter fencing, breach of security doors, to create a false alarm in order to observe reactions);
- k. Person(s) attempting to smuggle contraband through an access control point (e.g., airport screening center, security entrance point at a court of law, sports event, entertainment event);
- l. Person(s) making, or attempting to make, suspicious purchases, such as large amounts of otherwise legal materials (e.g., pool chemicals, fuel, fertilizer, potential explosive device components);
- m. Person(s) attempting to acquire sensitive or restricted items or information (e.g., plans, schedules, passwords);
- n. Person(s) attempting to acquire illegal explosives, components thereof, or precursor agents;
- o. Person(s) attempting to obtain an illegal chemical agent (e.g., nerve agent, blood agent, blister agent);
- p. Person(s) attempting to obtain an illegal biological agent (e.g., anthrax, ricin, Ebola virus, smallpox virus);

- q. Person(s) attempting to acquire illegal radiological material (e.g., uranium, plutonium, hospital x-ray discards);
- r. Person(s) in possession of, or using, explosives for an illegal purpose;
- s. Person(s) in possession of, or using, an illegal chemical agent (e.g., dry ice bomb, chlorine, phosgene);
- t. Person(s) in possession of, or using, a biological agent for an illegal purpose (e.g., anthrax, ricin, Ebola virus, smallpox virus);
- u. Person(s) in possession of, or using, radiological material, for an illegal purpose (e.g., as a weapon);
- v. Person(s) attempting to acquire, or having possession of, a uniform without a legitimate cause (e.g., service personnel, police, fire/EMS, security officer uniform);
- w. Person(s) attempting to acquire, or having possession of, an official, or official-appearing vehicle (e.g., emergency or government vehicle), without a legitimate cause;
- x. Person(s) pursuing specific training or education which may indicate suspicious motives (e.g., flight training, weapons training);
- y. Person(s) in possession of a stockpile of unexplained currency;
- z. Person(s) in possession of multiple passports, personal identifications, and/or travel documents issued to the same person or containing the photograph of a single person under multiple names;
- aa. Person(s) espousing extremist views (e.g., verbalizing support of terrorism, inciting or recruiting others to engage in terrorist activity);
- bb. Person(s) bragging about affiliation or membership with an extremist organization;
- cc. Person(s) engaged in suspected coded conversations or transmissions (e.g., by email, radio, and telephone);
- dd. Person(s) displaying overt support of known terrorist networks (e.g., by maintaining posters of terrorist leaders);

- ee. Person(s) using, or in the possession of, a hoax/facsimile explosive device;
  - ff. Person(s) using, or in the possession of a hoax/facsimile dispersal device; and
  - gg. Person(s) in possession of, or engaged in the solicitation of, sensitive event schedules (e.g., for the National Mall, White House, presidential movement, dignitary movement).
8. Suspicious Activity Reporting System – Software system used to capture and analyze suspicious activity information from various sources, including, but not limited to law enforcement representatives (through iWatchDC until the law enforcement module is created in the Records Management System), critical infrastructure owners and operators (TrapWire), and citizens (iWatchDC).

#### IV. REGULATIONS

- A. Members shall collect, maintain and disseminate intelligence information in compliance with all applicable District of Columbia laws, rules, regulations and the "Privacy Policy Statement of Principles" included in Attachment A.
- B. Information collected in the Suspicious Activity Reporting System may be used only for a *bona fide* law enforcement and/or intelligence analysis purposes and/or for defense in civil or administrative actions brought against Metropolitan Police Department member(s) or the Metropolitan Police Department.
- C. Absent exigent circumstances, Personally Identifiable Information in the Suspicious Activity Reporting System may not be disseminated to persons or agencies outside the Metropolitan Police Department without the prior written approval of the Chief of Police or his/her designee.
- D. Personally Identifiable Information in the Suspicious Activity Reporting System shall be maintained for up to five (5) years from the date it was entered into the Suspicious Activity Reporting System, and may be retained for additional time periods when there is a determined need. However, at the conclusion of the five (5) year retention period, or at such a period of time when all perceived or determined use has lapsed, the Commanding Official/Director, Intelligence Fusion Division, shall ensure that the data are properly deleted.
- E. No provision of this General Order precludes, in any way, any member from taking immediate action during the commission of a criminal act, or in circumstances which require the immediate defense of life, regardless of the nature or origin. Members who receive reports of or observe suspicious

activity shall investigate and take appropriate police action, to include proper tactical responses and notifications.

## V. PROCEDURES

### A. iWatchDC

1. Members who obtain information concerning, or observe, suspicious activity shall, in all cases, enter the information into the iWatchDC website.
2. Members may access the iWatchDC website (<https://iwatchdc.dc.gov>) through a link on the MPD Intranet Homepage, Mobile Inside, and the Internet.
  - a. To access iWatchDC via the MPD Intranet Homepage or Mobile Inside, members shall click on "iWatchDC".
  - b. To access iWatchDC via the internet, members shall open an Internet browser and enter <https://iwatchdc.dc.gov> in the address bar.
3. Once in iWatchDC, members shall:
  - a. Click "Make a report".
  - b. Enter their contact information, and then click "Next".
  - c. Enter basic information about the incident (time it occurred, number of people involved, number of vehicles involved), then click "Next".
  - d. Enter the location of the suspicious activity in the "Address" field and click "Go".
  - e. Drag the indicator on the map to specify a more precise location, and then click "Next".
  - f. If a person was involved, enter information to describe that person, and then click "Next".
  - g. If a vehicle was involved, enter information to describe that vehicle, and then click "Next".
  - h. Enter a description of what they saw, including why they believe the activity was suspicious, and then click "Next".

- i. Upload any documents, photographs, videos, or audio files of the people, vehicles, or activity by clicking "Browse..." to upload them, and then click "Next".
    - j. Review the information they entered, and then click "Submit" when they are done.
  4. After submitting the information into iWatchDC, members shall immediately notify the Watch Commander in the Police District where the suspicious activity occurred.
  5. Members who record observations or reports of suspicious activity in their police notebook shall transfer this information into the iWatchDC website, prior to the completion of their tour of duty.
- B. Suspicious Activity Related to Contacts and Stops
  1. Members who in the course of their duties initiate a contact/stop requiring the preparation of a PD Form 76, with which suspicious activity is associated, shall report the contact/stop in the iWatchDC website including the CCN.

NOTE: Members are reminded that contacts may be initiated when the member reasonably believes that some investigatory inquiry into a situation is warranted. Contacts shall not be initiated merely because a person is "hanging around," "loitering," or "standing on the corner," unless the overall circumstances are such as would reasonably arouse the curiosity, concern, or suspicion of the officer. Contacts shall not be conducted in a hostile or aggressive manner, nor as a means of harassing any person or attempting to coerce a person to leave an area.
  2. Members shall record in the "Comments" and/or "Narrative" Section of the contact/stop report as much detail as possible concerning the observations of, or information concerning, the involved party(s) and the circumstances, including any involved vehicle, weapon, suspicious package/item and potential target of the suspicious activity, such as a government building, embassy, corporation, business, or office of an elected official.
  3. Members shall immediately notify the Watch Commander in the Police District of occurrence upon the initiation of the contact/stop report.
  4. Members who complete a paper/notebook copy of the PD Form 76 involving associated suspicious activity shall transfer this information into the iWatchDC website prior to the completion of their shift.

5. Members are reminded that following a contact, members shall inform the contacted person:
  - a. A PD Form 76 will be completed;
  - b. The information contained within the PD Form 76 is not available to the public; and
  - c. The creation of the PD Form 76 does not signify or imply an arrest circumstance or involvement in criminal activity.

C. Suspicious Activity Related to Offense/Incident Report

1. Members who, as part of documenting an offense or incident, are completing a PD Form 251 in the Records Management System who need to report associated suspicious activity, shall also enter the information into the iWatchDC website.
2. Members shall record the CCNs obtained for the original PD Form 251 in the "Comments" section of the iWatchDC website.
3. Members shall record, in the iWatchDC website, as much detail as possible concerning the observations of, or information concerning, the involved party(s) and the circumstances, including any involved vehicle, weapon, suspicious package/item and potential target of the suspicious activity, such as a government building, embassy, corporation, business, or office of an elected official.
4. Members shall only enter Personally Identifiable Information (PII) in the name and address data fields. PII shall not be entered in the "Comments" Section in the iWatchDC website.
5. Members shall immediately notify the Watch Commander in the Police District where the suspicious activity occurred.
6. Members who complete a paper/notebook copy of the PD Form 251 involving associated suspicious activity shall transfer this information into an electronic PD Form 251 and enter the information into the iWatchDC website, prior to the completion of their shift.

## VI. ROLES AND RESPONSIBILITIES

A. District Watch Commanders shall:

1. Immediately confirm with the Command Information Center (CIC) when notified that information has been entered into iWatchDC.



2. Ensure that all members who obtain CCNs for suspicious activity or stops, or who complete a paper/notebook copy of a PD Form 251/PD Form 76 involving associated suspicious activity, transfer the information, as appropriate, into the iWatchDC website, prior to the end of their shift.
  3. Record in the PD Form 150 (Tour of Duty Supervisor's Report) the CIC confirmation (name/rank of member notified, date/time of notification, and related CCNs) and response by specialized units. Specialized units may include, but not be limited to, the Special Operations Division, Explosive Ordinance Unit (EOU); Intelligence Fusion Division (IFD); Joint Terrorism Task Force (JTFF); Investigative Services Bureau (ISB); and CIC.
- B. Supervisory officials shall:
1. Respond to, and personally review, all reports of suspicious activity (i.e., PD Forms 76 and 251) of their assigned personnel when a notification is made to, or response by, a specialized unit occurs.
  2. Ensure the response is adequate and that the report is complete, with all proper notifications having been made.
- C. The supervisor of the Criminal Intelligence Branch, Field Intelligence Group (FIG) will review all iWatchDC reports to ensure that the report is adequate and complete. If additional information is needed from the reporting member, the supervisor of the FIG will make arrangements to obtain the requisite information.
- D. The CIC shall alert the executive/command staff when a specialized unit is requested to respond to a report of suspicious activity (i.e., PD Form 76/iWatchDC).
- E. The Commanding Official/Director, Intelligence Fusion Division, shall ensure:
1. Procedures are established for reviewing suspicious activity reports (e.g., PD Forms 76) submitted into the iWatchDC website; and
  2. The suspicious activity reports (i.e., PD Forms 76; iWatchDC) are forwarded to the appropriate database for further analysis, review, and/or disposition.
- F. The Commanding Official/Director of the Metropolitan Police Academy shall provide training pertaining to the proper handling of suspected criminal or terrorism-related activity and Suspicious Activity Reporting Program measures as approved by the Chief of Police.

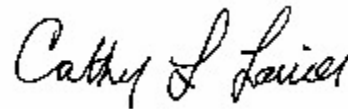
- G. The Assistant Chief, Homeland Security Bureau shall monitor compliance with the requirements of this General Order and recommend amendments as necessary.

**VII. CROSS REFERENCE**

General Order 304.10 (Police-Citizen Contacts, Stops and Frisks)

**VIII. ATTACHMENT**

Attachment A: Suspicious Activity Reporting Program, Privacy Policy, Statement of Principles



Cathy L. Lanier  
Chief of Police

CLL:PAB:MOC:CC:JC



# METROPOLITAN POLICE DEPARTMENT WASHINGTON, D.C.



## Suspicious Activity Reporting Program

### Privacy Policy Statement of Principles

---

This **Statement of Principles** governs the collection, maintenance, storage and dissemination of intelligence information by the Homeland Security Bureau, Intelligence Fusion Division and all other functions and personnel of the Metropolitan Police Department when their primary responsibility is gathering intelligence information.

In establishing this **Statement of Principles**, the Metropolitan Police Department provides for the legitimate needs of law enforcement within the limits created by constitutional and statutory protections which guarantee the rights: (1) Of privacy, (2) To receive, hold and express ideas, (3) To dissent freely, (4) To write and to publish, (5) To petition for the redress of grievances, and (6) To associate publicly and privately for any lawful purpose.

In order to protect the rights of individuals while providing for the effective prevention of criminal and terrorist activity: the Metropolitan Police Department affirms the following principles:

1. It is the policy of the Metropolitan Police Department to prohibit the use of illegal or unauthorized methods of collecting, maintaining or disseminating intelligence information. The Assistant Chief, Homeland Security Bureau, shall report to the Chief of Police any intelligence activity reasonably believed to be contrary to the scrupulous observation of this **Statement of Principles**.
2. The Metropolitan Police Department considers it both unnecessary and improper to maintain an intelligence file on any individual or organization unless the reasonable suspicion standard for an open intelligence investigation has been met.
3. Members shall not collect, maintain or disseminate intelligence information about an individual's race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity, family responsibilities, disability, matriculation, political affiliation, beliefs, or opinions unless such information is material to an approved investigation.

4. Members shall exercise due caution and discretion in the use of the intelligence information collected, maintained, and disseminated so as not to interfere with the lawfully exercised rights of any person.

## I. LIMITATIONS AND PROHIBITIONS

Members shall recognize and abide by all legal and policy requirements placed upon their investigations. In addition to the parameters established by this **Statement of Principles**, the following specific limitations and prohibitions apply to Metropolitan Police Department members and investigations:

1. No member may knowingly employ or direct any individual to illegally engage in the collection, maintenance or dissemination of intelligence data or information.
2. No member may act or knowingly engage another individual to act as an agent provocateur.
3. No member may employ the use of restricted electronic surveillance equipment without conforming to all related legal, regulatory, and Metropolitan Police Department requirements, including, but not limited to, those established in the DC Official Code, Title 6A DCMR (Police Personnel), and Metropolitan Police Department written directives.
4. Preliminary investigations shall not exceed one hundred twenty (120) days except as authorized by the Commanding Official/Director, Intelligence Fusion Division.

## II. PUBLIC ACCESS TO INFORMATION

- A. The Assistant Chief, Homeland Security Bureau may provide public access to intelligence documents collected in connection with this **Statement of Principles** unless those documents are exempt from production by DC Official Code § 2-534 (2001 Ed.) or by any other privilege recognized in the District of Columbia.
- B. In providing disclosure pursuant to requests made under this section, or other applicable law, each document shall be evaluated within the scope of each such request on an individual document-by-document basis.