



**U.S. Customs and  
Border Protection**

**FEB 15 2018**

MEMORANDUM FOR: Investigative Operations Division (IOD)

FROM: Erick K. Funn (b) (6), (b) (7)(C)  
Executive Director  
Investigative Operations Division

SUBJECT: Operational Use of Social Media for IOD

The purpose of this memorandum is to provide guidance to the IOD SAC Offices when IOD Special Agents use social media during the course of an investigation.

Effective February 12, 2018, DHS approved IOD's documentation which permits the use of social media in criminal and administrative investigations. All agents must read, acknowledge, and comply with the requirements in this memorandum, as well as, applicable DHS and CBP operational use of social media directives and Rules of Behavior. All agents must sign the attached Operational Use of Social Media for IOD Acknowledgement of Receipt. All agents must be mindful that pursuant to CBP Directive 1440-026A, Reporting Allegations of Misconduct dated April 17, 2017, or any superseding CBP Directive, any violation of a CBP Directive or policy shall be immediately documented and reported to the JIC.

**Operational Use of Social Media Investigations**

**General**

OPR IOD may use social media during the course of both criminal and administrative investigations. It is incumbent upon each SA to understand the below governing documents and comply when using social media for operational purposes. Direct any questions regarding the use of social media to an OPR IOD Headquarters Director.

SAs will conduct all social media investigations in accordance with the [CBP Operational Use of Social Media Directive 5410-003](#), the CBP Operational Use of Social Media Rules of Behavior, the [DHS Directive 110-01-001 "Privacy Policy for Operational Use of Social Media"](#), the approved IOD Criminal Investigations Social Media Operational Use Template, and the approved IOD Administrative Social Media Operational Use Template.

## Approval Process

**Special Agents:** Prior to using social media during the course of an investigation, SAs must complete the training on the [Operational Use of Social Media](#), located on Sharepoint. SAs must read and understand the IOP, the CBP Operational Use of Social Media Directive 5410-003, the CBP Operational Use of Social Media Rules of Behavior, and DHS Directive 110-01-001 "Privacy Policy for Operational Use of Social Media. Signed acknowledgements for the training and Operational Use of Social Media Rules of Behavior are kept in the SA's local personnel file, as well as forwarded to the CBP Privacy Office at (b) (7)(E)

Lastly, SAs must submit a request for approval online via (b) (7)(E). The online approval request shall be submitted every six months. The signed acknowledgements for the training and Operational Use of Social Media Rules of Behavior must be submitted annually after initial approval is received.

**First Level Supervisors:** Review requests for (b) (7)(E) of Social Media. Consider the purpose of the request and determine whether approval would serve an appropriate authorized purpose for an operational need that has been approved by the DHS Privacy Office through a Social Media Operational Use Template (SMOUT) and approve or deny such requests.

**Second Level Supervisors or Higher:** Review requests for (b) (7)(E) of social media. Consider the purpose of the request and determine whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the DHS Privacy Office through a SMOUT and approve or deny such requests.

## Documentation

All information collected through social media must be recorded in the appropriate system of record. In the case of OPR IOD, JICMS is the appropriate system of record. The information obtained must be documented in an ROI for each operational use of social media. Each ROI must contain the following information:

- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)

All information collected through social media must be protected to the same extent as other PII in JICMS and must follow any chain of custody requirements for that system, as appropriate.

## Types of Operational Use

IOD SMOUTS are approved for use in criminal and administrative investigations. SAs are permitted to use (b) (7)(E) techniques in relation to Social Media investigations.

(b) (7)(E)

CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission may conduct (b) (7)(E) of social media, after obtaining approval, if the research is necessary for an authorized purpose with a clear nexus to their assigned duties after a properly approved Template is in place.

(b) (7)(E)

(b) (7)(E)

**PROHIBITED SOCIAL MEDIA ENGAGEMENT BY SAs**

OPR IOD does not (b) (7)(E) and is not able to conduct (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Approved IOD employees using the CBP systems in furtherance of the CBP mission must comply with the specific terms for (b) (7)(E)

(b) (7)(E) as set forth in the CBP Operational Use of Social Media Rules of Behavior.

(b) (7)(E)

(b) (7)(E)

This requires approval from a second level supervisor or higher.

(b) (7)(E)

Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must identify themselves as associated with CBP by applying appropriate branding and disclaimers to distinguish the agency's activities from those of nongovernment actors. For example, Business Owners or Project Managers should add the CBP seal or emblem to the program's profile page on a social media website to indicate that it is an official agency presence.

(b) (7)(E)

(b) (7)(E)

This requires approval from a second level supervisor or higher.

(b) (7)(E)

Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must identify themselves as associated with CBP by applying appropriate branding and disclaimers to distinguish the agency's activities from those of nongovernment actors. For example, Business Owners or Project Managers should add the CBP seal or emblem to the program's profile page on a social media website to indicate that it is an official agency presence.

U.S. Customs & Border Protection  
Office of Professional Responsibility  
Investigative Operations Division

**Operational Use of Social Media for IOD  
Acknowledgement of Receipt**

As a CBP Special Agent/Investigator who is authorized to carry out the investigative functions of the Office of Professional Responsibility, you are required to comply with and be thoroughly familiar with all aspects of the attached IOD memorandum on Operational Use of Social Media for IOD.

You have been provided a complete copy of the *IOD* memorandum on Operational Use of Social Media for IOD and the opportunity to discuss the contents with your supervisor or other management officials.

By signing this statement, you acknowledge that you have read, understand, and agree to comply with all parts and aspects of the *IOD* memorandum on Operational Use of Social Media for IOD.

\_\_\_\_\_  
Employee's Name (Printed)                      Employee's Signature                      Date

\_\_\_\_\_  
Employee's Duty Location

\_\_\_\_\_  
Supervisor's Name (Printed)                      Supervisor's Signature                      Date

This signed acknowledgment shall be included in the employee's local personnel file, subject to IOD Inspection Program review. The acknowledgement form shall also be forwarded by the supervisor to (b) (7)(E) \_\_\_\_\_.