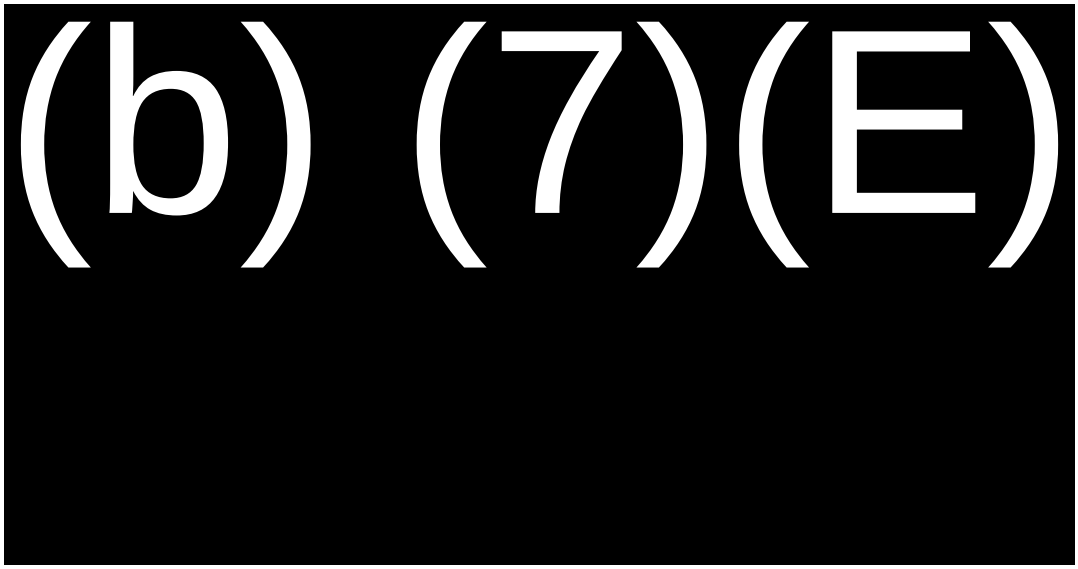
U.S. Customs and Border Protection

Interim Standard Operating Procedure for CBP Access to Operational Use of Social Media

I. **Purpose**: This Interim Standard Operating Procedure (SOP) for CBP Access to Operational Use of Social Media establishes the implementation process for U.S. Customs and Border Protection (CBP) employees and contractors to access social media for operational purposes. Implementation will occur through coordination between the Privacy and Diversity Office and Office of Information and Technology.

II. **Authorities/References**:
   a. DHS Directive 047-01, "Privacy Policy and Compliance" (July 7, 2011)
   b. DHS Instruction 047-01-001, "Privacy Policy and Compliance" (July 25, 2011)
   c. DHS Directive 110-01, "Privacy Policy for Operational Use of Social Media" (June 8, 2012)
   d. CBP Directive 2120-010, "Privacy Policy, Compliance, and Implementation" (January 2, 2015)
   e. CBP Directive 5410-003, "Operational Use of Social Media" (January 2, 2015)
   f. Memorandum from the Deputy Secretary to Component Heads, "Designation of Component Privacy Officers" (June 5, 2009

III. **Definitions**:
   a. 

   b. *Masked Monitoring* means using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation to conduct research or general, operational awareness. Masked monitoring includes logging in to social media, but does not include engaging or

interacting with individuals on or through social media (which is defined as Undercover Engagement).

c. *Operational Awareness* means information gathered from a variety of sources, that when communicated to emergency managers and decision makers, can form the basis for incident management or readiness state decision making.

d. *Operational Use* means use of social media to collect personally identifiable information (PII) for the purpose of enhancing general operational awareness, investigating an individual in a criminal, civil, or administrative context, assist in making a benefit determination about a person, assist in making a personnel determination about a CBP employee or contractor, assist in making a suitability determination about a prospective CBP employee or contractor, or for any other official CBP purpose that has the potential to affect the rights, privileges, or benefits of an individual or CBP employee or contractor. Operational use does not include the use of search engines for general Internet research, the use of social media for professional development (e.g., training and continuing education), or the use of social media for facilitating internal meetings, assigning or trading work shifts, or other internal administrative efficiencies.

e. *Overt Research* means collecting information from social media without logging in or otherwise interacting with individuals through social media. Overt research does not include creating identities or credentials on social media, nor does it include concealing a government affiliation to conduct research or general, operational awareness (e.g., non-DHS affiliated IP address).

f. *Overt Engagement* means logging in to social media using DHS/CBP-branded credentials or otherwise indicating an official agency presence and engaging or interacting with individuals on or through social media.

g. *Overt Monitoring* means logging in to social media using DHS/CBP-branded credentials or otherwise indicating an official agency presence, but does not include engaging or interacting with individuals on or through social media (which is defined as Overt Engagement).

h. *Personally Identifiable Information (PII)* means 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.

i. *Social Media* means the sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social media takes many different forms, including but not limited to web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies. This definition does not apply to internal Department intranets or applications.

j. *Social Media Operational Use Template (SMOUT)* means the document that each office must submit to CBP Privacy Office for approval by the DHS Privacy Office that describes the current or proposed category of operational use(s) of social media, identifies the appropriate authorities for the current or proposed category of use(s), describes what PII, if any, is or would be collected (and from whom or by what method), how that information is used, where the information would be stored, and if that collection, storage, and usage is consistent with the current SORN, and any appropriate training. The SMOUT is used to identify information technology systems, technologies, rulemaking, programs, or pilot projects that involve collecting PII from social media for the current or proposed category of use(s) and to assess whether there is a need for additional Privacy Compliance Documentation. Through submission to the CBP Privacy Office, templates will be reviewed and adjudicated by the DHS Chief Privacy Officer, and every three years thereafter for accuracy.

k. *Undercover Engagement* means using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation, to engage or interact with individuals on or through social media.

IV. Procedures:

a. A CBP employee completes an online application through the (b) (7)(E) , requesting access to social media using the (b) (7)(E) form. Information in the online application must include a detailed business justification as to why the employee needs access to social media through (b) (7)(E) .

b. After review of the (b) (7)(E) application, the CBP Office of Information and Technology, Security Operations Center (CBP SOC), forwards information from the (b) (7)(E) name of employee, phone number, email address, location, supervisor information, and business justification, to the CBP Privacy Office's email address (b) (7)(E) for review and CBP Privacy Officer approval.

c. The CBP Privacy Officer and/or designee verifies that the individual has completed the mandatory training and signed the CBP Operational Use of Social Media Rules of Behavior, and reviews the provided business justification to determine if it is appropriate for the requested use and is authorized by an approved Social Media Operational Use Template (SMOUT).

The determination made by the CBP Privacy Office and provided to CBP SOC will be one of the following:

(i) *Approved*: all required training has been completed, a copy of the signed Rules of Behavior has been provided to CBP Privacy, and the business

justification is in accordance with assigned job duties and authorized by an approved SMOUT.

(ii) *Additional information required*: employee has either not completed training or signed the Rules of Behavior (or both), or additional information is needed regarding the business justification.

(iii) *Disapproved*: the business justification is not in accordance with assigned job duties and/or an approved SMOUT.

d. After receipt of the CBP Privacy Office's determination, the CBP SOC forwards the application to CBP Office of Information and Technology, Chief Information Security Officer (CISO), for further review.

The CISO verifies approval of the individual's request with the employee's Supervisor based on the type of use as outlined by the requirements described below and responds to CBP SOC with either an approval or disapproval:

i. First Line Supervisors:
   a. Review requests for Overt Research use of social media, considers the purpose of the requests, and determines whether granting approval would serve an appropriate authorized purpose for an operational need; and
   b. Approve or deny the requests.

ii. Second Level Supervisors, or higher:
   a. Review requests for Overt Monitoring, Overt Engagement, and Masked Monitoring use of social media, considers the purpose of the request, and determines whether granting approval would serve an appropriate authorized purpose for an operational need; and
   b. Approve or deny the requests.

iii. Supervisors in the Senior Executive Service, and Second Level Supervisors at the GS-15 Level, or higher, delegated by the Office of Internal Affairs Director of Investigations Division:
   a. Review requests for Undercover Engagement use of social media, considers the purpose of the request, and determines whether granting approval would serve an appropriate authorized purpose for an operational need; and
   b. Approve or deny the requests.

e. After receipt of the CISO's review and response (approval or disapproval), CBP SOC forwards the (b) (7)(E) to the DHS SOC for final approval and implementation of access to the (b) (7)(E)

f. After implementation by the DHS SOC, CBP SOC forwards the (b) (7)(E) number and date of implementation to the CBP Privacy Office for accounting purposes.