U.S. CUSTOMS AND BORDER PROTECTION DIRECTIVE

CBP DIRECTIVE NO. 5410-003 **DATE: January 2, 2015**
ORIGINATING OFFICE: OC-PDO
REVIEW DATE: January 2018

SUBJECT: OPERATIONAL USE OF SOCIAL MEDIA

1 PURPOSE

To assign responsibilities and establish general rules of behavior for the operational uses of social media for U.S. Customs and Border Protection (CBP), in compliance with all applicable statutes, regulations, and Department of Homeland Security (DHS) or government-wide policies.

2 SCOPE

This Directive applies to all CBP employees, contractors, and to persons using CBP systems in furtherance of the CBP mission. However, this Directive does not apply to the operational use of social media for communications and outreach with the public authorized by the DHS Office of Public Affairs. Moreover, this Directive does not apply to the operational use of social media to the extent that CBP is utilizing social media for situational awareness purposes on behalf of the DHS National Operations Center.

3 POLICY

It is the policy of CBP to collect, maintain, use, and disseminate PII through the operational use of social media only when there is an authorized need to know the information. CBP will protect PII collected during the authorized operational use of social media, and comply with DHS privacy policy, applicable privacy laws, federal government-wide policies, and other statutory authorities. The procedures set forth in this directive must be followed before PII may be collected by CBP through the use of social media, stored in a CBP system of records, or shared with another party.

4 AUTHORITIES/REFERENCES

4.1 Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 3501 note];

4.2 Title 5, U.S. Code, Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended];

4.3 Title 6, U.S. Code, Section 142, "Privacy Officer;"

4.4 Title 8, U.S. Code, Section 1363a;

4.5 Title 19, U.S. Code, Section 2081;

4.6 Title 44, U.S. Code, Chapter 35, Subchapter III, "Information Security" [The Federal Information Security Management Act of 2002, as amended (FISMA)];

4.7 Title 6, C.F.R., Chapter 1, Part 5, "Disclosure of records and information;"

4.8 DHS Delegation 13001, "Delegation to the Chief Privacy Officer;"

4.9 DHS Sensitive Systems Policy Directive 4300A;

4.10 DHS Directive 047-01 "Privacy Policy and Compliance" (July 7, 2011) and Instruction 047-01-001 "Privacy Policy and Compliance" (July 25, 2011);

4.11 DHS Directive 110-01 "Privacy Policy for Operational Use of Social Media" (June 8, 2012) and Instruction 110-01-001 "Privacy Policy for Operational Use of Social Media" (June 8, 2012);

4.12 CBP Memorandum "Privacy Compliance and U.S. Customs and Border Protection" (February 10, 2012);

4.13 CBP Memorandum "Executive Agent Appointment for a CBP Integrated Intelligence, Surveillance, and Reconnaissance (ISR) Capability" (July 20, 2011);

4.14 CBP Information Systems Security Policies and Procedures Handbook 1400-05D; and

4.15 CBP Delegation Order 11-001 "Delegation of Authority for Discipline and Adverse Actions" (April 6, 2011).

5 DEFINITIONS

5.1 ***Business Owner*** means the CBP employee responsible for the planning and operation of a CBP project, operation, or program that collects PII.

5.2 ***Fair Information Practice Principles*** means the policy framework adopted by DHS in Directive 047-01, "Privacy Policy and Compliance," regarding the collection, use, maintenance, disclosure, deletion, or destruction of PII.

5.3 ***Individual*** means a natural person, including United States citizens and aliens (e.g., lawful permanent residents and nonimmigrants).

5.4 ***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, below).

5.5 **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.

5.6 ***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).

5.7 ***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.

5.8 ***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, above).

5.9 ***Operational Use*** means use of social media to collect 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.

5.10 ***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.

5.11 ***Privacy Compliance Documentation*** means any document required by statute or by the Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to the Social Media Operational Use Template (SMOUT), Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), Notices of Proposed Rulemaking for Exemption from

certain aspects of the Privacy Act (NPRM), and Final Rules for Exemption from certain aspects of the Privacy Act.

5.12 ***Privacy Liaison*** means the CBP employee responsible for serving as a point of contact and initial identifier of privacy issues in a CBP office.

5.13 ***Project Manager*** means the CBP employee or contractor in the Office of Information and Technology or other Office responsible for building and technically maintaining an authorized system with privacy implications.

5.14 ***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 take 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.

5.15 ***Social Media Operational Use Template (SMOUT)*** means the document that each office must submit to the CBP Privacy and Diversity Office for approval by the DHS Privacy Office that describes the current or proposed category of operational uses(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 Template is used to identify information technology systems, technologies, rulemakings, 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 and Diversity Office, templates will be reviewed and adjudicated by the DHS Chief Privacy Officer, and every three years thereafter for accuracy.

5.16 ***System of Records Notice (SORN)*** means the official public notice of a DHS or CBP system of records as required by the Privacy Act of 1974 (as amended). The SORN identifies (1) the purpose for the system of records, (2) the individuals covered by information in the system of records, (3) the categories of records maintained about individuals, (4) the source of the records and (5) the ways in which the information is generally shared by DHS and CBP. The SORN also provides notice of the mechanisms available for individuals to exercise their Privacy Act rights to access and correct the PII that DHS and CBP maintains about them.

5.17 ***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.

6 RESPONSIBILITIES

6.1 All CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission are responsible for:

6.1.1 Using social media for operational purposes only when activities are authorized by statute, executive order, regulation, or policy and approved through the procedures in this Directive;

6.1.2 Using only government-issued equipment, internet connections authorized to access social media through the DHS/CBP network (i.e., no "stand-alone" connections), and government-approved accounts when engaging in the operational use of social media, unless otherwise specifically authorized and approved;

6.1.3 Use screen names or identities that indicate an official DHS/CBP affiliation and use DHS/CBP email addresses to open accounts used when engaging in the operational use of social media, unless otherwise specifically authorized and approved;

6.1.4 Accessing publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information, unless otherwise specifically authorized and approved;

6.1.5 Respecting individuals' privacy settings and access only information that is publicly available unless the individual whose information the employee seeks to access has given consent to access it, or as otherwise authorized and approved;

6.1.6 Collecting only the minimum PII necessary for the proper performance of their authorized duties;

6.1.7 Protecting PII as required by the Privacy Act and DHS privacy policy;

6.1.8 Documenting operational use of social media, including date, site(s) accessed, information collected, and how it was used in the same manner that CBP would document information collected from any source in the normal course of business;

6.1.9 Complying with DHS Directive 110-01 and Instructions 110-01-001, with privacy policies and procedures issued by the DHS Chief Privacy Officer, and with applicable CBP policies on operational use of social media; and

6.1.10 Completing training on the operational use of social media and signing the CBP Operational Use of Social Media Rules of Behavior before any social media use and annually thereafter, if operational use of social media is a continuing requirement in the performance of their responsibilities.

6.2 **The Assistant Commissioner for the Office of Information and Technology** is responsible for:

6.2.1 Providing web technology services, security, and technical assistance for the operational use of social media within CBP; and

6.2.2 Ensuring that any technical system providing Masked Monitoring and/or Undercover Engagement accurately documents user login credentials and profiles and maintains sufficient audit logs for each user.

6.3 **The Assistant Commissioner for the Office of Intelligence and Investigative Liaison** is responsible for serving as the Business Owner governing the provision of intelligence, surveillance, and reconnaissance (ISR) capabilities, including Masked Monitoring and Undercover Engagement of Social Media. This includes ensuring Masked Monitoring and Undercover Engagement of Social Media meet operational and intelligence needs and providing direction to Office of Information and Technology (OIT) regarding intelligence related technologies available to be leveraged for all aspects of ISR to be used within CBP.

6.4 **The CBP Privacy Officer** is responsible for:

6.4.1 Maintaining an accurate accounting of all CBP categories of operational use of social media using the SMOUT to identify collection and use of PII, the authority for such collection and use, and any other attendant privacy impacts, and ensuring CBP implements DHS privacy policy with respect to the operational use of social media;

6.4.2 Coordinating with CBP Business Owners and Project Managers, as appropriate, together with the DHS Chief Privacy Officer and the Office of Chief Counsel to complete a SMOUT and any other required Privacy Compliance Documentation for (1) for all proposed categories of operational use of social media, and (2) for any changes to the categories of operational use of social media ;

6.4.3 Developing and reviewing CBP policies and directives related to Operational Use of social media, and CBP Rules of Behavior consistent with the adjudicated Template, to ensure compliance with DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies;

6.4.4 Overseeing CBP privacy training for operational use of social media and providing educational materials, consistent with privacy training for operational use of social media developed by the DHS Chief Privacy Officer;

6.4.5 Reviewing documentation required in 6.1.8 to ascertain compliance with this Directive as needed; and

6.4.6 Collaborating with the DHS Chief Privacy Officer in conducting Privacy Compliance Reviews.

6.5 **CBP Office of Chief Counsel** is responsible for:

6.5.1 Providing advice to Business Owners or Project Managers, as appropriate, to ensure that appropriate authority exists to engage in categories of operational use of social media before CBP employees engage in those uses, and to ensure that the Template generally documents that authority;

6.5.2 Providing legal guidance to the CBP Privacy Officer, Business Owners, or Project Managers, as appropriate, in the drafting of CBP Operational Use of Social Media Rules of Behavior Rules of Behavior for operational use of social media.

6.6 **CBP Business Owners and Project Managers**, as appropriate, are responsible for:

6.6.1 Coordinating with the CBP Privacy Officer to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any operational use of social media;

6.6.2 Coordinating with the CBP Privacy Officer and the Office of Chief Counsel to prepare draft Templates and CBP Operational Use of Social Media Rules of Behavior, and, as appropriate, all Privacy Compliance Documentation required when proposing, developing, or implementing or changing any category of operational use of social media;

6.6.3 Monitoring the design, deployment, operation, and retirement of programs involving the operational use of social media to ensure that the use of PII, if any, is limited to those uses described in the Privacy Compliance Documentation;

6.6.4 Ensuring oversight mechanisms, including, for example, audit trails and/or privacy compliance reviews, as appropriate, are built into the design of programs and systems involving the operational use of social media;

6.6.5 Coordinating with the CBP Privacy Officer to establish administrative, technical, and physical controls for storing and safeguarding PII consistent with DHS privacy, security, and records management requirements to ensure the protection of PII from unauthorized access, disclosure, or destruction in the course of operational use of social media; and

6.6.6 Supporting the CBP Privacy Officer in developing and implementing privacy procedures and job-related privacy training to safeguard PII in operational uses of social media.

6.7 Supervisors are responsible for:

6.7.1 Reviewing request(s) for Overt Research of social media, considering the purpose of the request, and determining whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the Chief Privacy Officer through a SMOUT; and

6.7.2 Approving or denying such requests.

6.8 Second Level Supervisors, or higher, are responsible for:

6.8.1 Reviewing request(s) for Overt Monitoring, Overt Engagement, and Masked Monitoring of social media, considering the purpose of the request, and determining whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the Chief Privacy Officer through a SMOUT; and

6.8.2 Approving or denying such requests.

6.9 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 Investigative Operations Division are responsible for:

6.9.1 Reviewing request(s) for Undercover Engagement of social media, considering the purpose of the request, and determining whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the Chief Privacy Officer through a Template; and

6.9.2 Approving or denying such requests.

7 PROCEDURES

7.1 General Procedures

7.1.1 Each CBP Office must complete a Template. That Template must identify which parts of the Office engages in operational use of social media, the type of operational use and the purposes achieved through the program(s). This must be completed before engaging in any operational uses of social media, including Overt Research, Overt Monitoring, Overt Engagement, Masked Monitoring, or Undercover Engagement.

7.1.2 The Office must provide the completed Template to the CBP Privacy and Diversity Office via its Privacy Liaison (if the office has a designated Privacy Liaison) or directly to the CBP Privacy Officer.

7.1.3 The CBP Privacy and Diversity Office, with appropriate coordination with the Office of Chief Counsel, must review and approve the Template before submitting it to the DHS Chief Privacy Officer for review and approval.

7.1.4 If directed by the DHS Chief Privacy Officer, the CBP Privacy Officer and the Office must complete any Privacy Compliance Documentation to address the particular operational use of social media stated in the completed Template.

7.1.5 The Office must complete any other additional steps outlined in Sections 7.2, 7.3, 7.4, 7.5, or 7.6 of this Directive, as appropriate.

7.1.6 Authorized CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission who plan to use social media under this directive, after a Template is approved, must complete training regarding the Operational Use of social media. These persons must also sign and comply with the CBP Operational Use of Social Media Rules of Behavior before engaging in any of the activities listed in Sections 7.2, 7.3, 7.4, 7.5, or 7.6 of this Directive, and annually thereafter.

7.1.7 All CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission who have created and used social media log-in credentials or profiles for operational use prior to the promulgation of this Directive must submit a request as specified in Sections 7.2, 7.3, 7.4, 7.5, or 7.6 of this Directive and must also complete training and sign the CBP Operational Use of Social Media Rules of Behavior within 90 days of the implementation date of this Directive to continue utilizing the credential or profile.

7.1.8 All information collected through social media must be recorded in the appropriate system of records, including date, site(s) accessed, information collected, and how the information was used, in the same manner that CBP would document information collected from any source in the normal course of business. All information collected through social media must be protected in the appropriate system of records to the same extent as other PII in that system and follow any chain of custody requirements for that system, as appropriate.

7.2 Overt Research

7.2.1 CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission must obtain approval from a CBP supervisor before conducting Overt Research of social media.

7.2.2 CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission may conduct Overt Research 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.

7.3 Overt Monitoring of Social Media

7.3.1 CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission must obtain approval from a second level CBP supervisor, or higher, before Overt Monitoring of social media.

7.3.2 Requests for approval for Overt Monitoring of social media must describe the authorized mission, the CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission authorized to use social media, the nexus to their assigned duties, the social media and any log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program.

7.3.3 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.

7.4 Overt Engagement of Social Media

7.4.1 CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission must obtain approval from a second level CBP supervisor, or higher, before Overt Engagement of social media.

7.4.2 Requests for approval for Overt Engagement of social media must describe the authorized mission, the CBP employees contractors, and persons using CBP systems in furtherance of the CBP mission authorized to use social media, the nexus to their assigned duties, the social media and any log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program.

7.4.3 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.

7.5 Masked Monitoring

7.5.1 (b) (7)(E) [redacted]

7.5.2 Approval of Masked Monitoring of social media must be re-approved every [redacted]

7.5.3 [redacted]

7.5.4 Requests for Approval for Masked Monitoring of social media must describe the authorized purpose for an operational need, the CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission authorized to conduct the Masked Monitoring of social media, the nexus to their assigned duties, the social media sites to be accessed, log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program. [redacted]

7.5.5 Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must comply with the specific terms for "Undercover Operational Use of Social Media and the Public Internet" as set forth in the attached CBP Operational Use of Social Media Rules of Behavior.

7.6 Undercover Engagement of Social Media

7.6.1 CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission may obtain approval to use social media for Undercover Engagement only when necessary for authorized law enforcement purposes with a clear nexus to their assigned duties and in conformance with existing undercover operations policies.

7.6.2 [redacted]

7.6.3 [redacted]

7.6.4 Approval of Undercover Engagement of Social Media must be re-approved every [redacted] through the procedures in 7.6.2.

7.6.5 Requests for Approval for Undercover Engagement of Social Media must describe the authorized purpose for an operational need, the CBP employees, contractors, and to persons using CBP systems in furtherance of the CBP mission authorized to use social media under cover, the social media sites used, log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program. [redacted]

(b) (7)(E) [redacted].

7.6.6 Approved employees, contractors, and to persons using CBP systems in furtherance of the CBP mission must comply with the specific terms for "Under cover Operational Use of Social Media and the Public Internet" as set forth in the attached CBP Operational Use of Social Media Rules of Behavior.

8 PRIVACY INCIDENT HANDLING

8.1 Unauthorized use of social media will be considered a Privacy Incident.

8.2 In accordance with the DHS Privacy Incident Handling Guidance, all Privacy Incidents are to be immediately reported, as appropriate, to the DHS Security Operations Center (SOC) or CBP Computer Security Incident and Response Center (CSIRC) for review, investigation, mitigation, and remediation, as necessary.

8.3 Pursuant to CBP Delegation Order 11-001 "Delegation of Authority for Discipline and Adverse Actions" (April 6, 2011), unauthorized use of social media may be grounds for appropriate disciplinary action, as determined by the employee's supervisor.

9 MEASUREMENT/INSPECTION

9.1 CBP's Office of Internal Affairs, Management Inspections Division, shall develop and periodically, or at a minimum once each calendar year, administer an inspection mechanism to determine whether CBP Offices are in full compliance with this Directive.

10 DISCLOSURE

10.1 This Directive is for internal use only and may not be shared with the public.

11 NO PRIVATE RIGHT CREATED

This document is for internal CBP use only, and does not create or confer any rights, privileges, or benefits for any person or entity.

R. Gil Kerlikowske
Commissioner
U.S. Customs and Border Protection