1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

Rachel Levinson-Waldman
Brennan Center For Justice
1140 Connecticut Ave NW
Suite 1150
Washington, DC 20036

January 17, 2018

Dear Rachel Levinson-Waldman,

Your CBP FOIA request is complete. Please use the following password to open your documents:

Levinson-Waldman054815

Your documents will be sent in a separate email.

We noticed that you do not have a FOIAonline account. When submitting future requests, please create one by taking the following steps:

- Simply go to your search engine (i.e., google, etc.) and type FOIAonline, then hit enter, that will take you to the FOIAonline site.
- From there, press the green button on the right "Create an Account" and follow the prompts to create a FOIAonline account.
- Make sure when creating your account you use the same email address that you provided when submitting your original FOIA request –that way the email addresses in your original FOIA request can be synched with the FOIAonline account you create.

Submitting a FOIA request online is the preferred method (vs. postal mail) for many reasons:

- You immediately receive a unique FOIA tracking number and acknowledgment that your FOIA request was received by CBP.
- You can track your FOIA request any day/any time through your FOIAonline account.
- When responsive records become available, you receive an email letting you know records can be viewed via your FOIAonline account,
- You can view all of your historical FOIA requests via the "dashboard" in your FOIAonline account.

In the future, please use your FOIAonline account to submit future FOIA requests to CBP. Please note that all FOIA requests for official travel records on an individual must include 1) the subject's name, 2) the subject's date of birth, and 3) third party consent. If this information is not provided with the original FOIA request, it will be considered "insufficient", and will not be processed.

Sincerely,

Andrea D. Banks Bertrand
U.S. Customs and Border Protection

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, *Privacy Policy for Operational Use of Social Media.* For the purposes of the Management Directive and this template, "Operational Use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings. The following uses of social media are exempt from the Management Directive and are not subject to this requirement[1]:

a) Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue and DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications);

b) The conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended.

This template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

---

[1] Gathering information by the Office of Operations Coordination and Planning (OPS) to enhance situational awareness is exempt from this requirement and is covered by the existing PIA: DHS/OPS/PIA-004(d) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update.

DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer. Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

SUMMARY INFORMATION

Date submitted for review:

Name of Component: Customs and Border Protection

Contact Information: (b) (7)(E), (b) (7)(C), (b) (6) **Director, Passenger Targeting, Office of Intelligence and Investigative Liaison** (b) (7)(E), (b) (6), (b) (7)(C)

Counsel[2] Contact Information: (b) (7)(E), (b) (7)(C), (b) (6), **Office of Chief Counsel, Enforcement Section**

IT System(s) where social media data is stored:

- **Automated Targeting System- Targeting Framework.**

Applicable Privacy Impact Assessment(s) (PIA):
DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012. Per the ATS PIA, ATS maintains the official record "for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information;"

Applicable System of Records Notice(s) (SORN):
DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297. Categories of records includes "Operational and analytical reports and/or projects developed that may include public source information and/or classified information obtained by users/analysts for reference or incorporation into the report or project."

- **Analytical Framework for Intelligence**

DHS/CBP/PIA-010 – Analytical Framework for Intelligence (AFI), June 1, 2012. Per the AFI PIA § 2.1 Identify the information the project collects, uses, disseminates, or maintains: "... DHS AFI analysts may upload information that the user believes is relevant to a project, including information publicly available on the Internet."

DHS/CBP-017 – Analytical Framework for Intelligence System June 7, 2012 77 FR 13813. Per the Record Source Categories: "Additionally, AFI permits analysts to upload and store any information from any source including public and commercial sources, which may be relevant to projects, responses to RFIs, or final intelligence products."

[2] Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.

DHS OPERATIONAL USE OF SOCIAL MEDIA

SPECIFIC QUESTIONS

1. **Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.**

The personnel anticipated to use social media under this SMOUT include (b) (7)(E) This SMOUT encompasses both Overt Research and Masked Monitoring. CBP personnel who receive specific prior supervisory approval may access and review information from any online source to gain information that is related to those individuals (b) (7)(E) Information gained through these operations may only be used consistent with the legal authorities of CBP. For example, this may include (b) (7)(E) Any information gained via social media as revealed by Internet search engine queries may be retained, as deemed relevant by a trained CBP analyst, in records of examinations or case files in the Automated Targeting System's Targeting Framework (ATS-TF) or the Analytical Framework for Intelligence. The data will be captured in the Targeting Framework and will indicate which user uploaded/input the information and the date/time when it was input. Other information relating to the (b) (7)(E), will also be documented. This information may be stored in AFI or ATS-TF.

2. **Based on the operational use of social media listed above, please provide the appropriate authorities.**

Under 235 of the Immigration and Nationality Act and its implementing regulations CBP Officers and Border Patrol Agents have several enforcement authorities and responsibilities associated with inspections at a port of entry. 8 U.S.C. § 1225; *see also* 8 CFR 287.2 (stating that a special agent in charge, port

director, or chief patrol agent shall initiate an investigation when he has reason to believe there has been a criminal immigration violation); 8 CFR 287.4 (stating that several positions within Border Patrol may issue subpoenas to be used in criminal or civil investigations); 8 CFR 287.9 (stating that Border Patrol agents must obtain a search warrant prior to conducting a search in a criminal investigation unless a specific exemption to the warrant requirement is authorized by statute or recognized by courts). *See also* 19 U.S.C. § 482, 1467, 1496, 1582, and 1589a, and 19 CFR Part 162.

a) **Has Counsel listed above reviewed these authorities for privacy issues and determined that they permit the Program to use social media for the listed operational use?**

☒ Yes. ☐ No.

3. **Is this use of social media in development or operational?**

☐ In development. ☒ Operational. Date first launched: Unknown

4. **Please attach a copy of the Rules of Behavior that outline the requirements below.**

Attached are the CBP Directive and Rules of Behavior.

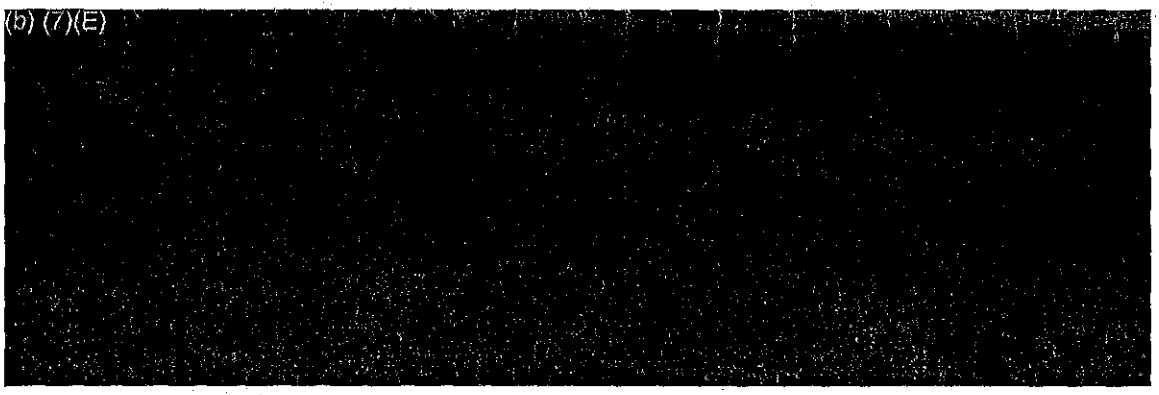
5. **Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:**

a) *Equipment.* Use only government-issued equipment when engaging in the operational use of social media;

☒ Yes. ☐ No. If not, please explain:

b) *Email and accounts.* Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

(b) (7)(E)



c) *Public interaction.* Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

☒ Yes. ☐ No. If not, please explain:

Yes- personnel with prior approval may conduct Masked Monitoring (b) (7)(E) to access social media in order to gain information related to those individuals who (b) (7)(E)

d) *Privacy settings.* Respect individuals' privacy settings and access only information that is publicly available;

☒ Yes. No. If not, please explain:

Yes – When applicable CBP employees utilized Overt Research, CBP personnel will only access information that is displayed openly, without logging in.

Yes - When applicable CBP employees utilized Masked Monitoring, authorized CBP personnel may access information that is available by (a) logging in to the social media or (b) logging in to the social media and gaining permission to view information without bearing CBP log-on information. All information accessed by CBP personnel through Masked Monitoring is done without any interaction by the individuals being monitored, including without the individual accepting CBP personnel's initiation to access data he/she makes available to those who are generally members of the site or forum. However, masked monitoring does not involve, for example, "friending," "fanning," or "liking," and as such, privacy settings are respected.

e) *PII collection*: Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

☒ Yes. ☐ No. If not, please explain:

f) *PII safeguards.* Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

☒ Yes. ☐ No. If not, please explain:

g) *Documentation.* Document operational use of social media, including date, site(s) accessed, information collected and how it was used.

☒ Yes. ☐ No. If not, please explain:

h) *Training*. Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials provided by the DHS Privacy Office. Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

☒ Yes. ☐ No. If not, please explain:

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No. If not, please explain:

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: May 13, 2015

NAME of the DHS Privacy Office Reviewer: Debra L. Danisek

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

PIA: DHS/CBP/PIA-006 ATS

SORN: DHS/CBP-006 ATS

DHS Privacy Office Determination

☐ Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

☐ Program has not yet met requirements to utilize social media for operational purposes.

- ☐ Program authorities do not authorize operational use of social media.
- ☐ Rules of Behavior do not comply. <Please explain analysis.>
- ☐ Training required.

Additional Privacy compliance documentation is required:

- ☒ A PIA is required.
  - ☐ New.
  - ☐ Updated. <Please include the name and number of PIA to be updated here.>
- ☒ A SORN is required:
  - ☐ New.
  - ☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

CBP's use of social media for Operational Awareness is compliant with the DHS social media directive MD 110-01-011.

This SMOUT is intended to address Overt Research and Masked Monitoring. The ATS PIA referenced references CBP's use of information on the internet. The CBP Directive on the Operational Use of Social Media, CBP defines Overt Research and Masked Monitoring as follows:

- 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).
- 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).

(b) (7)(E)

[redacted]