The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, 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.

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

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: 06.11.13

Name of Component: U.S. Citizenship and Immigration Services, Fraud Detection and National Security Directorate (FDNS)

Contact Information: (b)(6)

Counsel[2] Contact Information: (b)(6)

(b)(6)

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

Applicable Privacy Impact Assessment(s) (PIA):

DHS/USCIS/PIA-013(a) - Fraud Detection and National Security Directorate (FDNS)

Applicable System of Records Notice(s) (SORN):

DHS/USCIS/PIA-013 - Fraud Detection and National Security Data System (FDNS-DS)

DHS/USCIS/ICE/CBP-001 - Alien File, Index, and National File Tracking System of Records November 21, 2013, 78 FR 69864

DHS/USCIS-006- Fraud Detection and National Security Records (FDNS) August 8, 2012, 77 FR 47411

[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.**

   Information from social media sources will be viewed and gathered by USCIS Fraud Detection and National Security (FDNS) officers during **background and administrative investigations** for cases involving possible fraud, national security, or public safety concerns.

   During the adjudication of immigration benefits, USCIS officers may discover indicators of potential fraud, criminal, public safety, or national security concerns. Cases where these concerns are identified are referred to local FDNS Immigration Officers (FDNS IOs) for administrative investigation. After completing an administrative investigation, officers will either provide the results to the referring adjudicator, who adjudicates the application or petition on its merits, or refer the case to ICE for removal or criminal prosecution. This USCIS administrative review during adjudication is foundational to future criminal prosecution.

   FDNS IOs follow detailed guidance when handling cases involving potential fraud, criminal, public safety, or national security concerns. Additional security and background checks are performed. USCIS records, documents, and materials may be reviewed for consistency with material and information provided by the applicant. While initial concerns may be resolved with these efforts alone, additional information from outside sources is often required.

   The internet is a resource that provides access to subscription data sources and publicly available information. Some publicly available information resides on social media websites. USCIS requires the ability to consider that information as it may contradict information provided to USCIS by the applicant. Information from social media also enables USCIS to build lines of inquiry when requesting evidence and during in-person interviews.

   As with all derogatory information uncovered by USCIS that may have an impact on adjudication, applicants will have the opportunity to explain or refute any adverse information discovered through social media research.

   As noted in the 2012 FDNS Privacy Impact Assessment, in compliance with *DHS Directive 110-01, Privacy Policy for Operational Use of Social Media and Instruction 110-01-001*, FDNS IOs will be permitted to access social media sites when conducting administrative investigations only after they have completed initial, training on use of social media and signed the "Rules of Behavior" form. FDNS IOs will then complete refresher training and sign the Rules of Behavior annually. When conducting official government business, FDNS IOs may not

establish accounts on social media sites using fictitious names or information, or use personal accounts for official government business. FDNS IOs must use government-issued equipment to access social media. FDNS IOs cannot communicate with users of social media sites, and may only passively review information. Further, any information, whether it is derogatory or not, found on a social media site that is used in an investigation must be printed and saved in appropriate systems of records, including but not limited to the applicant's alien file and the Fraud Detection and National Security Data System (FDNS-DS).[3]

As noted above, USCIS FDNS IOs functioning under this Social Media Operational Use Template will never create fictitious names or use personal accounts for official government business. FDNS IOs will never directly interact with social media users. They will always use their official government email address when an account must be created to access a social media site, but they will not place their official title or agency affiliation in their screen names. A screen name that includes agency affiliation presents potential hazards to personnel and may hamper administrative investigations by:

* Providing untraceable and unidentifiable persons who may be interested in harming the Department of Homeland Security and its employees the ability to associate specific personnel with their DHS employer;

* Encouraging those who would intentionally mislead officers by sharing false information;

* Alerting an individual to the fact that they are being scrutinized by DHS. While de-confliction with law enforcement agencies is always undertaken by USCIS to avoid interference with Law Enforcement investigations,[4] USCIS may be the first USG entity to identify information that suggests an individual may be engaged in fraudulent or criminal behavior or a risk to national security and/or public safety.

Examples of information that can be gathered through social media include, but are not limited to:

- Addresses (Pertinent to relationship verification for family-based benefits).
- Stated relationships (Pertinent to relationship verification for family-based benefits).
- Biographical data (Pertinent to multiple benefit and action determinations).
- Educational and vocational attainment (Pertinent to employment based benefits).
- Professional and business involvement and associations (Pertinent to employment based benefits).
- Travel information (Pertinent to multiple benefit and action determinations).

[3] Privacy Impact Assessment for the Fraud Detection and National Security Directorate, DHS/USCIS/PIA-013(a), July 30, 2012.
[4] In accordance with the September 25, 2008 *Memorandum of Agreement between USCIS and ICE on the Investigation of Immigration Benefit Fraud.*

- Corporate, school and company information—many utilize social media pages rather than commercial websites (Pertinent to multiple benefit and action determinations).
- Resume postings (Pertinent to multiple benefit and action determinations).
- Blog and "Twitter" entries contrary to application information. (Pertinent to multiple benefit and action determinations).
- Location information and street-views of specific addresses: May suggest an address is not a business/industry, not a residence, not a school, not a law office, not a place of worship, or not industrial., etc. (Pertinent to multiple benefit and action determinations).
- An organization's stated purposes and activities (Pertinent to terrorist and/or other inadmissibility grounds in multiple benefit and action determinations).
- An organization's stated membership (Pertinent to determining an individual's past activity, location or membership in a group, which may then concern national security and/or other inadmissibility grounds in benefit determinations

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

- Homeland Security Act of 2002, as amended, Pub. L. No. 107-296, 116 Stat. 2135 (2002)
- Immigration and Nationality Act of 1952, as amended, § 101, 103
- 8 U.S.C. § 1101, 1103, 1155, 1184, 1324c, and 1357, Powers of immigration officers and employees
- 8 C.F.R. §§ 103.1, 103.2(b)(16)(i) and (ii)
- DHS Delegation No. 0150.1, Delegation to the Bureau of Citizenship and Immigration Services [USCIS]

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

USCIS has accessed general websites, applications and web-based tools since its inception. The agency will not implement the use of social media sites such as Facebook, YouTube and Twitter pending until after approval of this Template by the DHS Privacy Office, the development and implementation of USCIS Social Media policy, and the conduct of related privacy and operational training.

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

(See Accompanying FDNS 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;

☒ Yes. ☒ No. If not, please explain:

Yes, and No. Employees will always use DHS email addresses to open accounts used when engaging in operational use of social media. Screen names will not indicate an official DHS affiliation but employees will always use their own, true names when creating online screen names that will not indicate an official DHS affiliation.

A screen name that includes agency affiliation presents potential hazards to personnel and may hamper administrative investigations by:

* Providing untraceable and unidentifiable persons who may be interested in harming the Department of Homeland Security and its employees the ability to associate specific personnel with their DHS employer;

* Encouraging those who would intentionally mislead officers by sharing false information;

* Alerting an individual to the fact that they are being scrutinized by DHS. While de-confliction with law enforcement agencies is always undertaken by USCIS to avoid interference with Law Enforcement investigations,[5] USCIS may be the first USG entity to identify information that suggests an individual may be engaged in fraudulent or criminal behavior or a risk to national security and/or public safety.

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:

[5]In accordance with the September 25, 2008 *Memorandum of Agreement between USCIS and ICE on the Investigation of Immigration Benefit Fraud.*

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

☒ Yes. ☐ No. If not, please explain:

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:

Mechanisms are (or will be) in place to verify that users have completed training.

☒ 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: 8/1/2014**

NAME **of** the DHS Privacy Office Reviewer: (b)(6)

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.

☒ Covered by existing PIA. DHS/USCIS/PIA-013(a) - Fraud Detection and National Security Directorate (FDNS)

☐ New.

☐ Updated. <Please include the name and number of PIA to be updated here.>

☒ A SORN is required:

☐ Covered by existing SORN. DHS/USCIS-006 - Fraud Detection and National Security Records (FDNS) August 8, 2012, 77 FR 47411

☐ New.

☒ Updated. DHS/USCIS/ICE/CBP-001 – Alien File, Index, and National File Tracking System of Records, November 21, 2013, 78 FR 69864

DHS PRIVACY OFFICE COMMENTS

This SMOUT covers the use of social media by the USCIS FDNS Immigration Officers (IO) during background and administrative investigations for cases involving potential fraud, national security, or public safety concerns. The DHS Privacy Office (PRIV) finds that USCIS provided sufficient documentation to demonstrate compliance with the requirements of Management Directive 110-01.

FDNS IOs will follow the standard Rules of Behavior provided in DHS Instruction 110-01-001 with the exception of the requirement to use screen names or identities that indicate an official DHS affiliation. With supervisor approval, FDNS IOs may use a screen name that does not indicate an official DHS affiliation when the use of a DHS affiliation would make the subject or other material witness aware of the existence of an ongoing investigation or would jeopardize investigative efforts. For auditing and accountability purposes, USCIS must maintain a list of all such employees and their associated screen names. However, FDNS IOs must use their own names and official DHS email addresses to create online accounts.

The FDNS PIA provides PIA coverage for FDNS IO use of social media for administrative investigations. The FDNS PIA acknowledges that FDNS IOs may conduct searches of social media sites when conducting administrative investigations after the IO has completed annual training on the use of social media and signed rules of behavior. In the PIA, FDNS also committed to completing a policy for the use of social media prior to using social media for operational purposes.

Any information, whether or not that information is derogatory, that is collected from a social media site and used as part of an investigation is saved in the individual's A-File and electronically recorded in FDNS-DS. The A-File SORN covers the social media information placed in an individual's A-File. The A-File SORN should be updated to include publicly available information on the internet as a record source category, but this update is not required before FDNS IOs may access social media. The FDNS SORN covers information stored in FDNS-DS.