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

Contact Information: Donald Hawkins, Chief Privacy Officer, USCIS (b)(6)

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

(b)(6)

IT System(s) where social media data is stored: Some information may be stored in FDNS-DS, but most retained information is stored in non-electronic form, such as the A-File, or in an A-File that will later be digitized.

Applicable Privacy Impact Assessment(s) (PIA):

- DHS/USCIS/PIA-016, USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum
- DHS/USCIS/PIA-003(a) - Integrated Digitization Document Management Program (IDDMP)
- DHS/USCIS/PIA-025, Reengineered Naturalization Casework System(RNACS)
- DHS/USCIS/PIA-015, Computer Linked Application Information Management System 4 (CLAIMS 4)
- DHS/USCIS/PIA-027(a), Refugees, Asylum, and Parole System and the Asylum Pre-Screening System
- DHS/USCIS/PIA-044, Fraud Detection and National Security Directorate
  DHS/USCIS/PIA-045, Deferred Action for Childhood Arrivals
- DHS/USCIS/PIA-031- Citizenship and Immigration Data Repository (CIDR)

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

- DHS/USCIS/ICE/CBP-001 - Alien File, Index, and National File Tracking System of Records
- DHS/USCIS-002 - Background Check Service
- DHS/USCIS-006 - Fraud Detection and National Security Records (FDNS)
- DHS/USCIS-007 - Benefits Information System

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

- DHS/USCIS-008 - Refugee Access Verification Unit
- DHS/USCIS-010 - Asylum Information and Pre-Screening
- DHS/USCIS-012 - Citizenship and Immigration Data Repository (CIDR)

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.**

USCIS uses social media, as defined in the Privacy Policy, to gather information for the purpose of **Benefits Determinations** and in support of administrative investigations into alleged violations of the immigration laws. This use of social media, involves gathering information through reviewing social media sites, monitoring chat rooms, and reviewing comments posted on websites. This information is gathered to assist in **Benefits Determinations** by Immigration Services Officers (staff engaged in adjudications and/or background check activities); Asylum and Refugee Officers; and other USCIS employees engaged in the process of benefits determinations. This information is used in the same manner as information gathered from non-Internet and non-social media sources such as information gathered in person, on the phone, or through research of hard copy documents.

During the benefit determination process, USCIS reviews indicators of potential fraud and/or criminal, public safety, or national security concerns, any of which may lead to a finding that an applicant is ineligible for a particular benefit or other immigration action.

USCIS officers and support personnel routinely use a variety of government and commercial databases to determine when submitted information and documentation may require additional verification. The use of social media, allows USCIS to gather information to assist in benefit determinations.

USCIS may use social media when determining the best way to manage petitions and applications involved in large fraud schemes that are under investigation by law enforcement entities. USCIS may also use social media to isolate fraud indicators for use in the identification of fraud trends across application and petition types. These functions are Benefits Determinations functions that may sometimes occur after adjudication, when large scale fraud has been identified and past applications (as well as current) are involved.

Applicants will have the opportunity to explain or refute any adverse information discovered through social media.

Examples of information that can be gathered through social media include:

- Address reconciliation (Pertinent to relationship verification for family based benefits).
- Biographical Pages (Pertinent to multiple benefit and action determinations).
- Educational and Vocational Attainment (Pertinent to employment based benefits).
- Professional and Business Involvement & Associations (Pertinent to employment based benefits).
- 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, 208
- 8 U.S.C. § 1101, 1103, and 1357, Powers of immigration officers and employees

- 8 C.F.R. § 2.1, Authority of the Secretary of Homeland Security; 8 CFR §§ 208, 208.30 and 208.31.
- Section 203 of the Nicaraguan Adjustment and Central American Relief Act (NACARA § 203), in accordance with 8 CFR § 240.60.
- 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 has not implemented the use of social media websites such as Facebook, YouTube, Twitter, MySpace, and Hi5 pending approval of this Template by the DHS Privacy Office.

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

(See Accompanying USCIS Social Media 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:

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:

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.

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.

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.

☒ DHS/USCIS/PIA-003(a) Integrated Digitization Document Management Program (IDDMP)

☐ New.

☒ Updated. DHS/USCIS/PIA-016 Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3); DHS/USCIS/PIA-015(b) Computer Linked Application Information Management System (CLAIMS 4); DHS/USCIS/PIA-027 Refugees, Asylum, and Parole System and the Asylum Pre-Screening System; DHS/USCIS/PIA-45 Deferred Action for Childhood Arrivals (DACA)

☒ 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 for benefits determination purposes. DHS Privacy (PRIV) finds that USCIS has provided sufficient documentation to meet the requirements of DHS Directive 110-01.

USCIS will follow the standard Rules of Behavior provided in DHS Instruction 110-01-001 for use of social media for operational purposes when making benefits determinations. The standard Rules of Behavior apply to Immigration Services Officers (staff engaged in adjudications or background check activities), Asylum and Refugee Officers, and other USCIS employees engaged in the process of benefits determinations even when engaged in activities that, when done by a FDNS IO, would fall within the exemption for FDNS IOs. For auditing and accountability purposes, USCIS must maintain a list of all such employees and their associated screen names.

DHS Privacy requires USCIS to update the CLAIMS 3, CLAIMS 4, RAPS/APSS, and DACA PIAs to include social media as a source of information and to discuss any privacy risks and mitigations associated with the use of social media for benefits determination. The IDDMP PIA also provides coverage for USCIS's use of social media for benefits determination purposes. Any information, whether or not that information is derogatory, that is collected from a social media site and used as part of the benefits determination process will be saved in the individual's A-File and, when applicable, FDNS-DS. 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 USCIS may access social media for benefits determination purposes. The FDNS SORN covers information stored in FDNS-DS.