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.

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: 3/15/2015

Name of Component: U.S. Citizenship and Immigration Services

Contact Information: (b)(6)

Counsel[2] Contact Information:

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

Applicable Privacy Impact Assessment(s) (PIA):

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

[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.**

   USCIS may collect personally identifiable information from social media sources for purposes of incident management conducted by the USCIS Security Operations Center (SOC) and the Cyber Investigative Support Section (CISS), both within the Office of Information Technology, Information Security Division. USCIS SOC and CISS personnel are responsible for monitoring USCIS networks and incident response and investigations. For example, the SOC and CISS may use social media to identify who may be attempting to hack into USCIS systems. The USCIS SOC and CISS also provide assistance and cooperates with the DHS Security Operations Center and DHS Component Security Operations Centers when requested or when incident management concerns involve USCIS.

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

   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:

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

   (See Accompanying USCIS SNOC 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 their own, true names and DHS email addresses to open accounts used when engaging in operational use of social media. Employees will always use their own, true names in creating online screen names and site identities, but online screen names will not indicate an official DHS affiliation.

A screen name that includes agency affiliation presents potential hazards to personnel and may hamper general research, incident management and officer safety 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 persons to the fact that information is being scrutinized by DHS. USCIS may be the first USG entity to identify information that suggests a group or 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:

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: 3/15/2015**

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. <Please include the name and number of PIA here.>

☒ New.

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

☒ A SORN is required:

☐ Covered by existing SORN. <Please include the name and number of SORN here.>

☒ New.

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

DHS PRIVACY OFFICE COMMENTS

This SMOUT covers the use social media by the USCIS SOC and CISS to investigate threats to USCIS network security. As part of USCIS's use of social media, USCIS may collect PII. PRIV is unclear as to which IT system USCIS will be using to maintain this information.

USCIS 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, USCIS employees investigating threats to USCIS networks may use a screen name that does not indicate an official DHS affiliation when the use of a DHS affiliation would jeopardize investigative efforts. For auditing and accountability purposes, USCIS must maintain a list of all such employees and their associated screen names. However, as with the FDNS SMOUT, USCIS employees must use their own names and official DHS email addresses to create online accounts.

This collection is not covered under existing privacy compliance documentation. As required by the E-Government Act of 2002, USCIS must complete a Privacy Impact Assessment (PIA) before collecting PII under this initiative. This collection will be covered by the forthcoming DHS-wide Incidents PIA that is currently being drafted by the USCIS Privacy Office. USCIS must also complete and publish a System of Records Notice (SORN), as required by the Privacy Act of 1974. The SORN must be published in the Federal Register before USCIS may begin collecting PII for identifying and investigating USCIS network security issues using social media.