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: 06.11.13

Name of Component: US Citizenship and Immigration Services

Contact Information: (b)(6)

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

(b)(6)

IT System(s) where social media data is stored: Investigations Division Case Management System (IDCMS)

Applicable Privacy Impact Assessment(s) (PIA): IDCMS PIA - Currently in review at DHS Privacy

Applicable System of Records Notice(s) (SORN): DHS/ALL-020 – Department of Homeland Security Internal Affairs (73 FR 67529, November 18, 2008)

[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 used in the conduct of administrative investigations into allegations of employee misconduct.

During investigations into allegations of employee misconduct, USCIS seeks to acquire information that would prove or disprove the allegations. Allegations of misconduct that are investigated by USCIS may be submitted by USCIS employees directly to the Office of Security and Integrity's Investigations Division, or may be referred to USCIS by the DHS Office of Inspector General. Complainants (those submitting allegations of misconduct) often provide documentation supporting the allegation. Upon receiving an allegation of employee misconduct, USCIS' investigative staff then seeks to acquire information that would validate or verify any allegation. This information can take many forms (witness statements, physical evidence, personal and professional documents, etc.). The use of Social Media Internet sites, in particular, will enhance USCIS' investigative process, as a growing number of allegations of misconduct have a social media component such that access to social media sites would greatly aid the investigative process. As with other evidentiary sources, social media will not constitute the sole basis of an investigation, but will simply provide USCIS with an additional tool and allow it to gather more information during the course of an investigation. Consistent with the use of information acquired from other sources, USCIS employees who are the subjects of misconduct allegations will have the opportunity to explain or refute any information discovered on a social media site.

Some examples of evidence that can be gained through Social Media, and its potential pertinence to the investigative process:

- Biographical Pages (Pertinent to multiple investigative areas).
- Educational and Vocational Information (Pertinent to stated claims of employment).
- Resumes and Professional and Business Information, Involvement, and Associations (Pertinent to claims of outside activities).
- Photo, audio and video information from social media sites that support or refute an allegation.

- Blogs and other posts indicating location or actions (Pertinent to multiple investigative areas, such as to corroborate an individual's claim or rebuttal information).
- An individual's stated purposes and activities (Pertinent to national security and/or other investigative areas)
- An individual'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 background investigation and adjudication issues).

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

6 U.S.C. 273(a)(1)

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 OSI-INV 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.

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: 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-053, USCIS Investigations Division Case Management System (IDCMS) (currently in review with the DHS Privacy Office)

☐ New.

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

☒ A SORN is required:

☒ Covered by existing SORN. DHS/ALL-020 - Department of Homeland Security Internal Affairs April 28, 2014, 79 FR 23361

☐ New.

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

DHS PRIVACY OFFICE COMMENTS

This SMOUT covers the use of social media by the USCIS Office of Security and Integrity (OSI) Investigations Division (INV) for administrative investigations into allegations of employee misconduct. The DHS Privacy Office (PRIV) finds that USCIS provided sufficient documentation to demonstrate compliance with the requirements of DHS Directive 110-01.

OSI INV 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, OSI INV employees may use a screen name that does not indicate an official DHS affiliation when the use of a DHS affiliation presents a potential hazard to the employee or jeopardizes the investigation. For auditing and accountability purposes, USCIS must maintain a list of all such employees and their associated screen names.

OSI INV will document the use of social media in IDCMS. IDCMS has PIA coverage under the forthcoming IDCMS PIA that is currently in review with PRIV. The DHS Internal Affairs SORN covers the information contained within IDCMS.