The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-(b)(6);
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: October 12, 2012

Name of Component: U.S. Immigration and Customs Enforcement

Contact Information: (b)(6); (b)(7)(C) Deputy Privacy Officer, (202) 732-(b)(6)

Counsel[2] Contact Information: (b)(6); (b)(7)(C) Chief of Staff, (202) 732-(b)(6);

IT System(s) where social media data is stored: None

Applicable Privacy Impact Assessment(s) (PIA): None

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

DHS/ALL-017 – Department of Homeland Security General Legal Records

DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS)

DHS/ALL-025 - Department of Homeland Security Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security

[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.**

   As the definition of social media in the DHS Instruction 110-01-001 *Privacy Policy for the Operational Use of Social Media* (Privacy Policy) is drafted broadly so as to likely include general use of the Internet and as social media technology is ever changing and evolving, this template addresses ICE's use of the Internet, to include social media as defined in the Privacy Policy.

   ICE uses the Internet, including social media, for general research purposes. Use of the Internet, including social media, for general research purposes includes: (1) using the Internet, including social media, for legal purposes such as researching individuals or organizations who may be involved in lawsuits or other legal actions with ICE, judges adjudicating cases involving ICE, opposing counsel for cases involving ICE, and legal blogs and other online forums where legal issues of interest to ICE may be discussed; (2) using the Internet, including social media, to assist in gathering information on individuals who may meet with ICE officials to prepare ICE officials for those meetings; (3) using the Internet, including social media, to assist in gathering information on individuals who are suspected of attempting to hack into ICE systems, and (4) other general Internet, including social media, research.

   Category One: Legal Uses

   Most of ICE attorneys and support personnel's use of the Internet, including social media, is addressed in the four ICE Social Media Templates addressing: (1) Criminal and Administrative Immigration Law Enforcement, (2) Criminal Law Enforcement, (3) Undercover Criminal Law Enforcement, and (4) Administrative Law Enforcement. With regard to the use of the Internet, including social media, for other legal purposes, ICE attorneys and support personnel may view certain legal blogs such as SCOTUSblog[3] to keep informed on legal issues relevant to ICE. During the review of these sites, personally identifiable information, generally limited to an individual's name, may be viewed and in some cases recorded if relevant to a discussion or legal issue (whether author of a blog entry or individual mentioned in the blog). Further, while excluded from the definition of Operational Use, ICE attorneys and support personnel may also conduct general Internet research to find information on parties participating in litigation with ICE and judges

[3] SCOTUSblog is a legal blog focusing on discussions of recent developments in U.S. Supreme Court jurisprudence.

adjudicating cases involving ICE. For example, labor and employment attorneys may search the Internet to find relevant information on employees against whom allegations of misconduct have been made or who are otherwise involved in litigation against ICE.

Category Two: Meeting Preparations

ICE also uses the Internet, including social media, to research individuals with whom ICE employees may be meeting. For example, if the ICE Director is meeting with the head of the Virginia State Police, ICE employees may search on the Internet to gather biographical information, news reports, or other publicly available information on the head of the Virginia State Police so as to provide briefing materials to the Director. During these searches information may be pulled from public blogs and other publicly available online discussions.

Category Three: Security Operations Center

ICE also uses the Internet, including social media, to research individuals who are suspected of attempting to compromise ICE system integrity. In these instances the ICE Security Operations Center (SOC) performs searches in the process of performing cyber-incident investigations. During the course of incident response, SOC personnel sometimes will attempt to identify who may be attempting to hack ICE systems. To gain as much information as possible about the potential hacker, SOC personnel will investigate using major search engines and social media websites.

Category Four: General Research

Finally, ICE also uses the Internet, including social media, for general research purposes including researching individuals providing training to ICE so as to gather information on their background. This general Internet research is excluded from the definition of Operational Use but included here for transparency.

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
- Federal Information Security Management Act of 2002 (FISMA) (codified at 44 U.S.C. § 3541 *et seq.*)
- DHS Delegation No. 7030.2, Delegation of Authority to the Assistant Secretary of U.S Immigration and Customs Enforcement
- DHS Management Directive 140-01 Information Technology System Security
- DHS Sensitive Systems Policy Directive 4300A.

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.

The Internet has been in use at legacy agency since it was publicly available.

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

See Memorandum from John Morton, Use of Public Online Information for Non-Law Enforcement Work-Related Activities.

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. ☐ 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:

ICE employees should retain the contents of their use of the Internet, including social media, if they would have retained that content had it been written on paper. These contents should be preserved in accordance with office procedures in a manner authorized by the relevant records schedule.

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: **November 1, 2012**

NAME of the DHS Privacy Office Reviewer: (b)(6); (b)(7)(C)

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

DHS/ALL-017 – Department of Homeland Security General Legal Records

DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS)

DHS/ALL-025 - Department of Homeland Security Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security

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