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.

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

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: December 5, 2016

Name of Component: U.S Immigration and Customs Enforcement

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

Counsel[2] Contact Information: Adam Loiacono, Chief, Enforcement and Removal operations Law Division, OPLA; Erin Clifford, (A) Chief, Government Information Law Division, OPLA

IT System(s) where social media data is stored: TECS Case Management, Fugitive Case Management System, Enforcement Integrated Database, and Alien Criminal Response Information Management System

Applicable Privacy Impact Assessment(s) (PIA):

DHS/ICE/PIA-009 – Fugitive Case Management System (FCMS)

DHS/ICE/PIA-015 – Enforcement Integrated Database (EID)

DHS/ICE/PIA-011 – Visa Security Program Tracking System (VSPTS-Net)

DHS/ICE/PIA-020 – Alien Criminal Response Information Management System (ACRIMe)

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

DHS/ICE-009 – External Investigations

DHS/ICE-007 – Alien Criminal Response Information Management (ACRIMe) SORN

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

DHS/ICE-011 – Immigration and Enforcement Operational Records System (ENFORCE) SORN

DHS/ICE-012 – Visa Security Program (VSP) SORN

DHS/USCIS-ICE-CBP-001 – Alien File, Index, And National File Tracking System SORN

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 as defined in the Privacy Policy, for criminal and administrative immigration law enforcement purposes. (This template does not address the conduct of undercover operations in the context of criminal immigration law enforcement investigations. Those activities are covered by a separately submitted template that covers undercover investigations only.) This immigration law enforcement use of the Internet including social media, falls into the following four categories: (1) using the Internet, including social media, to assist in locating, arresting, and adjudicating individuals who may be amenable to removal under the Immigration and Nationality Act or are otherwise suspected of violations of U.S. immigration law and assisting other law enforcement agencies with investigations and adjudications related to individuals, (2) identify individuals who may be inadmissible to the United States under the Immigration and Nationality Act, (3) pre-operational, operational, and situational awareness uses related to officer safety or threats to the public at-large, and (4) to obtain information to assist in determining whether to exercise prosecutorial discretion.

   <u>Category One: Basic Criminal and Administrative Enforcement of the Immigration and Nationality Act</u>

   With regard to the use of the Internet, including social media, to locate and arrest individuals, ICE officers, agents, attorneys, and support personnel routinely use a variety of government and commercial databases to identify, locate, and arrest individuals who may be amenable to removal and meet ICE's current enforcement priorities. However, additional information not available in these databases is available on the Internet, including social media. The use of the Internet, including social media, will allow ICE to gather information that assists in identifying, locating, and arresting individuals wanted for crimes and/or who may be amenable to removal, and assisting other law enforcement agencies with investigations related to individuals where necessary and appropriate. It will also allow ICE attorneys who represent the agency in civil

immigration proceedings before the Executive Office for Immigration Review to conduct general and specific case research and preparation.

Category Two: Inadmissibility Recommendations under the Immigration and Nationality Act

ICE also uses the Internet, including social media, to identify individuals who may be inadmissible to the United States under the Immigration and Nationality Act. As a function of the Visa Security Program, ICE makes recommendations to the Department of State on the issuance and status of non-immigrant visas. ICE may collect information about non-immigrant visa applicants and their associated points of contact listed on their visa application in order to make these recommendations. This includes gathering information publicly available on the Internet, including social media, before and after visa approval. ICE may also collect information about non-immigrant visa holders. If derogatory information about a non-immigrant visa holder is uncovered, information may be shared with the Department of State and/or forwarded to the appropriate ICE Homeland Security Investigations field office for appropriate action depending on whether the non-immigrant visa holder has entered the United States.

Category Three: Officer and Public Safety

ICE also uses the Internet, including social media, for pre-operational/operational/situational awareness uses relating to officer safety or threats to the public at-large. Prior to conducting tactical enforcement operations or otherwise initiating contact with a subject, ICE agents, officers, or support personnel may collect information about the subject of the tactical enforcement operation. This includes gathering information publicly available on the Internet, including social media, such as firearms/weapons possession and relatives/associates who may reside with him. This information assists agents and officers with tactical planning activities such as: number of agents and officers required for the operation, any specialized equipment that may be necessary for the operation, and intelligence on when and where the operation should be conducted for agent and officer safety and tactical efficiency.

Category Four: Prosecutorial Discretion

Finally, ICE also uses the Internet, including social media, to gather information related to the possible exercise of prosecutorial discretion. Pursuant to Director Morton's June 17, 2011 memorandum relating to the exercising of prosecutorial discretion, ICE law enforcement personnel are expected to consider a number of factors when deciding whether to exercise prosecutorial discretion in various situations. Some of these factors include: whether the subject is a danger to the community or to national security, whether the subject is the primary caregiver to a minor, or a person with a physical or mental disability, a subject's educational and military background, a subject's ties and contributions to the community, whether the subject (or the subject's spouse) is pregnant or nursing, whether the subject or subject's spouse suffers from severe mental or physical illness. These factors can be difficult to ascertain using routine government and commercial databases and the use of the Internet

including social media serves as another tool to attempt to identify these unique factors. Similarly, some of these same factors may also apply when setting conditions of release from ICE custody. The Internet, including social media, provides a source of information that can be used to help determine when it is appropriate to release an individual from ICE custody.

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, U.S. Code Title 8
- DHS Delegation No. 7030.2, Delegation of Authority to the Assistant Secretary of U.S Immigration and Customs Enforcement
- ICE Delegation No. 0001, Delegation of Authority to the Directors, Detention and Removal and Investigations, and to Field Office Directors, Special Agents in Charge and Certain Other Officers of the Bureau of Immigration and Customs Enforcement
- 8 C.F.R. § 2.1, Authority of the Secretary of Homeland Security

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

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

See Memorandum from John Morton, Use of Public and Non-Public Online Information, June 28, 2012.

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:

Because the activities described in Question 1 are for immigration law enforcement purposes, the employees who engage in these activities will not identify themselves as ICE or DHS personnel, or law enforcement personnel. This is necessary to ensure the safety of law enforcement personnel, to avoid compromising law enforcement operations, to prevent tipping off individuals who are sought by law enforcement for violations of law, and to prevent disclosing litigation strategy and tactics.

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:

Because the activities described in Question 1 are for immigration law enforcement purposes, the employees who engage in these activities will not identify themselves as ICE or DHS personnel, or law enforcement personnel. This is necessary to ensure the safety of law enforcement personnel, to avoid compromising law enforcement operations, to prevent tipping off individuals who are sought by law enforcement for violations of law, and to prevent disclosing litigation strategy and tactics.

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:

Law enforcement personnel may not access restricted online sources or facilities absent legal authority permitting entry into private space.

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:

The applicable SORNs cited above are all exempted by Final Rules from the Privacy Act (e)(1) requirement (5 U.S.C. § 552a(e)(1)), which normally limits agencies to collecting only information about individuals that is relevant and necessary to accomplish a purpose of the agency required by statute or Executive Order. The exemption from the (e)(1) requirement is necessary to ensure the integrity of law enforcement investigations, as more fully detailed in the Final Rules.

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's rules of behavior stated that law enforcement personnel should retain the information they access on the Internet, including social media, if they would have retained that content had it been written on paper. These contents should be preserved in a manner authorized by ICE procedures governing the preservation of electronic communications.

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:

All ICE users will complete the necessary training when it is available.

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: January 3, 2017

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

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

PIA: DHS/ICE/PIA-009 Fugitive Case Management System (FCMS)

DHS/ICE/PIA-015 Enforcement Integrated Database (EID)

DHS/ICE/PIA-011 Visa Security Program Tracking System (VSPTS-Net)

DHS/ICE/PIA-020 Alien Criminal Response Information Management System (ACRIMe)

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

DHS/ICE-007 Alien Criminal Response Information Management System, February 14, 2013, 78 FR 10623

DHS/ICE-009 External Investigations, January 5, 2010, 75 FR 404

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, October 19, 2016, 81 FR 72080

DHS/ICE-012 Visa Security Program (VSP), September 30, 2009, 74 FR 50228

1. **Category of Use:**

☐ Law Enforcement Intelligence;

☒ Criminal law enforcement investigations;

☐ Background investigations;

☐ Professional responsibility investigations;

☐ Administrative or benefit determinations (including fraud detection);

☐ Situational awareness; and

☐ Other. <Please explain "other" category of use here.>

2. Has Component Counsel reviewed and determined that there is authority to engage in the above Category of Use?

☒ Yes. ☐ No.

3. Rules of Behavior Content: (Check all items that apply.)

a. *Equipment*.

☒ Users must use government-issued equipment. Equipment may be non-attributable and may not resolve back to DHS/US IP address.

☐ Users must use government-issued equipment. Equipment must resolve back to DHS/US IP address.

b. *Email and accounts*.

☒ Users do not have to use government email addresses or official DHS accounts online.

☐ Users must use government email addresses or official DHS accounts online.

c. *Public interaction*.

☐ Users may interact with individuals online in relation to a specific law enforcement investigation.

☒ Users may NOT interact with individuals online.

d. *Privacy settings*.

☐ Users may disregard privacy settings.

☒ Users must respect individual privacy settings.

e. *PII storage*:

☒ PII is maintained in an exempted Privacy Act System of Records.

Please list applicable SORN here: DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, November 21, 2013, 78 FR 69864; DHS/ICE-007 Alien Criminal Response Information Management System, February 14, 2013, 78 FR 10623; DHS/ICE-009

External Investigations, January 5, 2010, 75 FR 404; DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, October 19, 2016, 81 FR 72080; DHS/ICE-012 Visa Security Program (VSP), September 30, 2009, 74 FR 50228

☐ PII is maintained in a Privacy Act Systems of Records.

Please list applicable SORN here:

f. *PII safeguards.*

☒ PII is protected as required by the Privacy Act and DHS privacy policy.

☐ Only a minimal amount of PII is collected and safeguarded, consistent with DHS/OPS-004 – Publicly Available Social Media Monitoring and Situational Awareness Initiative.

g. *Documentation.*

☐ Users must appropriately document their use of social media, and collection of information from social media website.

☐ Documentation is not expressly required.

☒ ICE's rules of behavior stated that law enforcement personnel should retain the information they access on the Internet, including social media, if they would have retained that content had it been written on paper.

h. *Training.*

☒ All users must complete annual privacy training that has been approved by Component Privacy Officer. Training includes:

☒ Legal authorities;

☒ Acceptable operational uses of social media;

☒ Access requirements;

☐ Applicable Rules of Behavior; and

☒ Requirements for documenting operational uses of social media.

☒ 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, certification of training completion cannot be verified.

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.

☐ New.

☐ Updated.

☐ A SORN is required:

☐ New.

☐ Updated.

DHS PRIVACY OFFICE COMMENTS

PRIV determines that ICE has provided sufficient documentation to demonstrate compliance with the MD 110-01. DHS PRIV requests on a future update to DHS/ICE-012 VSP SORN, to include "Open source information news articles or other data available to the public on the Internet or in public records, including publicly available information from social media" as a Record source category to further specify social media use.