



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 requirement¹:

- 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:

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

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

Counsel² Contact Information: (b)(6); (b)(7)(C) Chief, Homeland Security Investigations Division, (202) 732-(b)(6); (b)(7)(C) Chief, Enforcement and Removal Operations Division, (202) 732-(b)(6);

IT System(s) where social media data is stored: TECS, ICE Child Exploitation Tracking System (CETS), General Counsel Electronic Management System (GEMS), Personnel Security Activities Management System (PSAMS)/Integrated Security Management System (ISMS), Joint Integrity Case Management System (JICMS), Enforcement Integrated Database (EID), and FALCON Search & Analysis System (FALCON-SA).

Applicable Privacy Impact Assessment(s) (PIA):

DHS/ICE/PIA-017 – Immigration and Customs Enforcement Child Exploitation Tracking System (ICE-CETS)

DHS/ICE/PIA-032 – FALCON Search & Analysis System (FALCON-SA)

DHS/ICE/PIA-002(a) – General Counsel Electronic Management System (GEMS)

DHS/ICE/PIA-020 – Enforcement Integrated Database (EID)

DHS/ALL/PIA-001(a) – Personnel Security Activities Management System (PSAMS)/Integrated Security Management System (ISMS)

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



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

DHS/ICE-006 – ICE Intelligence Records System (IIRS)

DHS/ICE 008 – Search, Arrest, and Seizure Records

DHS/ICE-009 – External Investigations

DHS/ALL-023 – DHS Personnel Security Management Records (PSAMS)

DHS/ICE-003 – General Counsel Electronic Management System (GEMS)

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

DHS/ALL-020 – DHS Internal Affairs Records



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 submission 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 law enforcement purposes. (This submission does not address the conduct of undercover operations in the context of criminal law enforcement investigations. Those activities are covered by a separately submitted document that covers undercover investigations only.) This criminal law enforcement use of the Internet, including social media, falls into the following three categories: (1) using the Internet, including social media, to assist in locating, arresting, and adjudicating fugitives and assisting other law enforcement agencies with investigations and adjudications related to the fugitive, (2) using the Internet, including social media, to assist in investigating, gathering evidence, and gathering criminal intelligence on criminal and potential criminal activity, and (3) pre-operational, operational, and situational awareness uses related to officer safety or threats to the public at-large.

Category One: Locating, Arresting, and Adjudicating Fugitives

With regard to the use of the Internet, including social media, to locate and arrest fugitives and criminals, ICE officers, agents, attorneys, and support personnel routinely use a variety of government and commercial databases to identify, locate, and arrest fugitives. These individuals could include members of the public or employees or contractors of ICE and CBP suspected of committing crimes or other forms of misconduct. 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 fugitives wanted for crimes and assisting other law enforcement agencies with identifying, locating, and arresting fugitives.

Category Two: Criminal Investigations and Law Enforcement Intelligence

ICE also uses the Internet, including social media, to assist in investigating, gathering evidence, and gathering law enforcement intelligence on criminal and potential criminal



activity. This use of the Internet, including social media, involves activities to gather information such as Internet searches, reviewing social media sites, monitoring chat rooms, and reviewing comments posted on websites. This information is gathered and used by ICE officers, agents, attorneys, and support personnel 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. Information gathered in this fashion may be used in criminal investigations of members of the public or employees or contractors of ICE and CBP.

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, and support personnel may collect information about the subject of the tactical enforcement operation. This information gathering includes information available on the Internet, including social media, such as firearms/weapons possession and relatives/associates who may reside with them. This information assists officers with tactical planning activities such as: number of 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 officer safety and tactical efficiency.

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)
- DHS Delegation No. 7030.2, Delegation of Authority to the Assistant Secretary of U.S Immigration and Customs Enforcement
- 19 U.S.C. § 1589a, Enforcement authority of customs officers
- 8 U.S.C. § 1357, Powers of immigration officers and employees

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 ICE's legacy agencies 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 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:

The nature of criminal investigations may require investigators to use non-government-issued equipment when engaging in criminal investigations. Investigators at times find themselves in rapidly evolving situations in the field that call for the use of adaptive measures. In situations where government-issued equipment is either not available, or is technologically insufficient to perform the required task at hand, investigators may need to rely on non-government-issued equipment. However, ICE is currently working to provide government-issued equipment so as to not require the use of non-government-issued equipment in these circumstances.

- 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 criminal 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. Where legal authority exists, law enforcement personnel may access restricted online information.

- 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 state 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:

Yes, employees self-certify that they have read and understood their Component Rules of Behavior.



**Homeland
Security**

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-(b)(6);
www.dhs.gov/privacy

Version date: June 12, 2012
Page 8 of
10

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: 11/6/2012

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.
 - DHS/ICE/PIA-017 – Immigration and Customs Enforcement Child Exploitation Tracking System (ICE-CETS)
 - DHS/ICE/PIA-032 – FALCON Search & Analysis System (FALCON-SA)
 - DHS/ICE/PIA-002(a) – General Counsel Electronic Management System (GEMS)
 - DHS/ICE/PIA-020 – Enforcement Integrated Database (EID)
 - DHS/ALL/PIA-001(a) – Personnel Security Activities Management System (PSAMS)/Integrated Security Management System (ISMS)
 - New.
 - Updated. <Please include the name and number of PIA to be updated here.>



A SORN is required:

Covered by existing SORN.

DHS/ICE-006 – ICE Intelligence Records System (IIRS)

DHS/ICE 008 – Search, Arrest, and Seizure Records

DHS/ICE-009 – External Investigations

DHS/ALL-023 – DHS Personnel Security Management Records (PSAMS)

DHS/ICE-003 – General Counsel Electronic Management System (GEMS)

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

DHS/ALL-020 – DHS Internal Affairs Records

New.

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

DHS PRIVACY OFFICE COMMENTS

The DHS Privacy Office determines that ICE has provided sufficient documentation to demonstrate compliance with the MD 110-01. The rules of behavior reference that Law Enforcement personnel shall follow ICE guidelines and procedures whether the activities are online or offline. ICE did not provide the “offline policy” that is referenced in the Rules of Behavior because it is very close hold and distribution is limited. This policy, referred to as the UC Ops Handbook governs ICE HSI undercover investigations. ICE PRIV has reviewed the document.

DHS PRIV also requested additional guidance on how the requirements to retain records were covered. ICE PRIV advised that Section 5 of the ICE principles covers the retention of records. DHS PRIV concurs.