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:

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, Homeland Security Investigations 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)

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

DHS/ICE-009 – External Investigations

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

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

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

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 template addresses ICE's use of the Internet, to include social media as defined in the Privacy Policy.

   With the enactment of the Homeland Security Act of 2002, Congress authorized ICE to conduct certified undercover investigative operations to obtain evidence or information concerning violations of laws enforced by ICE and stemming from the authorities of its legacy agencies, the U.S. Customs Service (USCS) and the Immigration and Naturalization Service (INS). Within ICE, investigations are only conducted by the Homeland Security Investigations (HSI) component and the Office of Professional Responsibility (OPR). The authority to certify undercover operations has been delegated to the Executive Associate Director of HSI and the Assistant Director for OPR. HSI and OPR may also engage in limited use of social media, when authorized, if an investigation does not otherwise warrant being placed under a certified undercover operation. These activities are detailed in the templates addressing Criminal Law Enforcement and Administrative Law Enforcement.

   Undercover activities and operations are undertaken for numerous potential objectives that include: (1) determining if a violation of law has occurred or is in progress; (2) identifying specific violations of law; (3) identifying criminal violators, conspirators, and their methodologies; (4) disrupting and/or dismantling criminal organizations; (5) locating the violation sites and equipment used; (6) locating assets for seizure and forfeiture; (7) obtaining evidence for prosecution; (8) determining the safest and most advantageous time to make arrests, execute search warrants, and make seizures; (9) identifying witnesses and cooperating individuals; (10) identifying associations between conspirators; (11) checking the reliability of sources of information and cooperating defendants; and (12) gathering intelligence that allows ICE management to evaluate threats, reallocate resources, and organize enforcement activity. ICE may collect personally identifiable information from or about individuals over the Internet, including via social media sites.

   The nature of undercover operations often requires an ICE-HSI or OPR criminal investigator to appear to be engaged in a criminal enterprise and to befriend or become business

associates with potential violators. This is crucial to the successful integration of undercover operatives with those who commit illegal acts. As part of a certified undercover investigation or operation, when authorized, undercover operatives may participate in activities that would constitute a crime under federal, state, or local law. This otherwise illegal activity includes, for example, the purchase of stolen or contraband goods, the purchase of illegal and/or fraudulent immigration documents, and the controlled delivery of drugs or other contraband that will not enter the commerce of the United States. ICE-HSI and OPR review and authorize, as appropriate, requests to engage in various otherwise illegal activities in furtherance of undercover operations. In the course of carrying out these authorized undercover activities, ICE-HSI or OPR criminal investigators may collect personally identifiable information using the Internet. Any of these activities may take place in part over the Internet, to include social media.

As the "rules" for undercover operations are different than non-undercover law enforcement work, and may require agents to engage in activities that would otherwise be considered prohibited or unauthorized, the rules of behavior for undercover criminal investigations are different than for non-undercover investigations.

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

USCS was vested with the authority to conduct certified undercover operations through the Anti-Drug Abuse Act of 1986, which enacted 19 U.S.C. § 2081; INS received similar authority through the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, specifically 8 U.S.C. § 1363a. With the enactment of the Homeland Security Act of 2002, these statutory authorities transferred to the newly created Department of Homeland Security (DHS) and were delegated to the Assistant Secretary of ICE in DHS Delegation Number 7030.2, "Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement," and further redelegated to the Directors of OI and OPR in ICE Delegation Order 04-002 entitled, "Authority to Certify the Exemption of Undercover Operations From Certain Laws Within U.S. Immigration and Customs Enforcement." ICE-HSI and OPR criminal investigators are granted their enforcement authority in 8 U.S.C. § 1357 and 19 U.S.C. § 1589a.

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:

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 undercover investigative purposes, the employees who engage in these activities have assumed an undercover identity and therefore will not identify themselves as ICE or DHS personnel, or law enforcement personnel in general. This is necessary to ensure the safety of law enforcement personnel, to avoid compromising undercover law enforcement operations, and to prevent tipping off individuals who are sought by law enforcement for violations of law.

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:

The nature of undercover criminal investigations may result in agents interacting with individuals who use social media sites. This interaction only takes place during authorized undercover investigations.

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 information they access on 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 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.

☒ 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:

DHS/ICE-009 – External Investigations

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

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

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.

ICE PRIV provided additional feedback on authorities to conduct UC Ops. Stating that ICE legal counsel advises that UC authority is granted specifically by Congress to identified federal LE agencies – we are one of 6 federal LE agencies that hold this authority. ICE's undercover authority is found in the authorities of its legacy agencies (USCS and INS), the statutory language for which has not been updated to reflect ICE as the current agency. However, through various transfer provisions in the Homeland Security Act and then a DHS delegation to ICE, the authority now rests with ICE. It is a bit convoluted, but here is how it breaks down:

- 19 U.S.C. 2081 "Undercover investigative operations of Customs Service." This is the authority held by the legacy USCS, and is now held by ICE HSI. For transfer of functions, personnel, assets, and liabilities of the United States Customs Service of the Department of the Treasury, including functions of the Secretary of the Treasury relating thereto, to the Secretary of Homeland Security, see sections 203(1), 551(d), 552(d), and 557 of Title 6, Domestic Security, and the Department of Homeland Security Reorganization Plan of November 25, 2002, as modified, set out as a note under section 542 of Title 6.

- 8 U.S.C. 1363a "Undercover investigation authority." This is the authority held by the legacy INS investigative arm, and is now held by ICE HSI. For discussion of transfer of function, see 8 U.S.C. 1551 note: "ABOLITION OF IMMIGRATION AND NATURALIZATION SERVICE AND TRANSFER OF FUNCTIONS The Immigration and Naturalization Service was abolished by section 291(a) of Title 6, Domestic Security, upon completion of all transfers from the Immigration and Naturalization Service as

provided for by chapter 1 of Title 6. Functions of the Commissioner of Immigration and Naturalization performed under the Border Patrol program, the detention and removal program, the intelligence program, the investigations program, and the inspections program, and all personnel, assets, and liabilities pertaining to such programs, were transferred to the Under Secretary for Border and Transportation Security of the Department of Homeland Security by section 251 of Title 6 and the Department of Homeland Security Reorganization Plan of November 25, 2002, as modified, set out as a note under section 542 of Title 6."

- DHS Delegation No 7030.2 "Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement." (link here: http://dhsconnect.dhs.gov/policies/Documents/7030.2%20Delegation%20of%20Authority%20to%20the%20Assistant%20Secretary%20for%20the%20Bureau%20of%20Immigration%20and%20Customs%20Enforcement.pdf) Section 2(A) delegates the 19 U.S.C. 2081 authority to ICE. Section 2(DD) delegates the 8 U.S.C. 1363a authority to ICE.

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.