The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

For Official Use Only

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); and

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. *See* DHS/OPS/PIA-004(d) Publicly Available Social Media Monitoring and Situational Awareness Initiative Update, *available at* 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: 4/30/2018

Name of Component: U.S. Citizenship and Immigration Services, Fraud Detection and National Security Directorate (FDNS)
Contact Information: Kevin T. Quinn, Kevin.T.Quinn@uscis.dhs.gov, 202-272-9106

Counsel[2] Contact Information:
Craig Symons Chief Counsel USCIS, 202 272-1400

IT System(s) where social media data is stored: FDNS-DS

Applicable Privacy Impact Assessment(s) (PIA):

DHS/USCIS/PIA-013-01 Fraud Detection and National Security Directorate (FDNS)

DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS)

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

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, September 18, 2017, 82 FR 43556

DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) August 8, 2012, 77 FR 47411

[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.**

   The USCIS Fraud Detection and National Security (FDNS) Officers view and gather information from social media sources for **background checks and administrative investigations** for cases involving possible fraud, national security, or public safety concerns.

   During the adjudication of immigration benefits, USCIS may discover indicators of potential fraud, criminal, public safety, or national security concerns. Cases where these concerns are identified are referred to local FDNS Immigration Officers (FDNS IOs) for administrative investigation. After completing an administrative investigation FDNS IOs will either provide the results to the referring adjudicator, who adjudicates the immigration service request on its merits, or refer the case to ICE for removal or criminal prosecution. This USCIS administrative review during adjudication is foundational to future criminal prosecution.

   FDNS IOs follow detailed guidance when handling cases involving potential fraud, criminal, public safety, or national security concerns. Additional security and background checks are performed. USCIS records, documents, and materials may be reviewed for consistency with material and information provided by the applicant.[3] While initial concerns may be resolved with these efforts alone, additional information from outside sources is often required.

   The internet is a resource that provides access to subscription data sources and publicly available information. Some publicly available information resides on social media websites. USCIS requires the ability to consider that information as it may contradict and/or substantiate information provided to USCIS by the applicant. Information from social media also enables USCIS to build lines of inquiry when requesting evidence and during interviews. As with all derogatory information uncovered by USCIS that may have an impact on adjudication, applicants will have

[3] As used in this document, the term applicant includes applicants, petitioners and requestors.

the opportunity to explain or refute any adverse information discovered through social media research if the applicant was unaware of that information.[4]

USCIS FDNS uses social media identifiers to conduct screening and vetting checks of applicants from publicly available information on social media. The social media reviews for applications are initiated with overt research. In certain instances when there are national security, public safety, or articulated and actionable fraud[5] concerns with an application and an overt research would compromise the integrity of an investigation, FDNS may use fictitious accounts[6] or identities to review the applicant's social media content that is publicly available to all users of the social media platform. Under no circumstance will DHS/USCIS violate any social media privacy settings, or directly engage in dialogue with the social media account holder.

As noted in the Public FDNS Directorate Privacy Impact Assessment (PIA) Update,[7] in compliance with DHS Directive 110-01, Privacy Policy for Operational Use of Social Media and Instruction 110-01-001, FDNS IOs will be permitted to access social media sites when conducting administrative investigations only after they have completed required training on the use of social media and signed the "Rules of Behavior" (RoB). FDNS IOs will then complete refresher training and sign the annually.

When conducting official government business, FDNS IOs may not provide false or misleading information about their identity to applicants, petitioners, or anybody else under investigation. However, FDNS IOs, with the approval of their supervisor, may use fictitious accounts or identities, where otherwise publicly-available information (information for which the accountholder has not invoked privacy protection settings) is only available to those who have an account with the service provider or social media platform, there are national security, public safety

---

[4] 8 CFR 103.2(b)(16)(i), requires that any derogatory information that an applicant is unaware of and that may be used in an unfavorable decision must be provided to the applicant in an interview, request for evidence, or notice of intent to deny. The applicant is given an opportunity to review and respond before a decision is made, provided an exemption does not apply (e.g., the information is classified).

[5] In accordance with the 2018 USCIS Fraud Detection Standard Operating Procedures, fraud will be deemed articulated if a subject has a nexus to an immigration related benefit and there is information to support a reasonable suspicion of fraud or willful misrepresentation of a material fact. Sufficient justification for opening a Case may also be articulated if there is reason to believe that, owing to fraud or willful misrepresentation, the subject is ineligible to transmit or receive a benefit requested under the INA. Fraud will be deemed actionable if it is within the scope of USCIS and an investigation by FDNS or an external entity (ICE, FBI, etc.) is likely to develop evidence that will support an administrative denial of an application, petition, request, criminal prosecution, or initiation of removal proceedings.

[6] Fictitious Account is defined as: using identities or credentials on social media that do not identify a DHS/USCIS affiliation, or otherwise concealing a government affiliation, to conduct research. Use of fictitious accounts also serves an essential operational security (OPSEC) mission by protecting USCIS employees and DHS IT systems from individuals or groups who may wish to do harm to one or both. Use of fictitious accounts or identities includes logging in to social media, but does not include engaging or interacting with individuals on or through social media.

[7] *See* DHS/USCIS/PIA-013-01(a) FDNS Directorate, *available at* www.dhs.gov/privacy.

concerns or articulated and actionable fraud, and overt research would compromise the integrity of an investigation. FDNS IOs must have approval from their supervisor not to use their official title or agency affiliation, and to use fictitious names and accounts to access social media sites. The FDNS IO names and associated fictitious account information are tracked and maintained by the FDNS IO's supervisor or manger. Cases involving use of fictitious accounts will be documented in FDNS-DS; and will be subject to routine audits by FDNS or USCIS leadership, the USCIS Office of Privacy, or the Office of Security and Integrity, either for routine audits or for-cause audits.

The approval process for the creation and use of fictitious accounts will be in accordance with the FDNS Implementation of DHS Delegation Number 15002 Standard Operating Procedures, which outlines the approval process for the creation and use of fictitious accounts, and the criteria for conducting routine and for cause audits. The SOP must be followed by FDNS supervisors and FDNS IOs.

FDNS IOs shall not use personal social media accounts for official government business. FDNS IOs must use government-issued equipment to access social media. FDNS IOs shall not communicate with users of social media sites and shall not engage other users in any way (e.g., "like" someone's comments), and may only passively review social media. Further, any information, whether it is derogatory or not, found on a social media site that is used in an investigation must be printed and saved in appropriate systems of records, including but not limited to the applicant's Alien file and the Fraud Detection and National Security Data System (FDNS-DS).[8]

As noted above, USCIS FDNS IOs will never directly interact with social media users. In most cases, a fictitious account will not be created using an official government email address to access a social media site, unless authorized by the FDNS leadership. Instead, USCIS will be using phone numbers provided by USCIS OIT. If account creation requires more information than can be provided by USCIS OIT, no account will be created. FDNS IOs will not place their official title or agency affiliation in their screen names. This practice will not inhibit the agency's ability to perform auditing and accountability. A screen name that includes an officer's true name or 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; or

[8] *See* DHS/USCIS/PIA-013(a) FDNS-DS, *available at* www.dhs.gov/privacy.

- Alerting an individual to the fact that they are being scrutinized by DHS. While de-confliction with law enforcement agencies is undertaken by USCIS to avoid interference with Law Enforcement investigations,[9] USCIS may be the first U.S. Government entity to identify information that suggests an individual may be engaged in fraudulent or criminal behavior or a risk to national security and/or public safety.

Examples of information that can be gathered through social media include, but are not limited to:

- Physical addresses (Pertinent to relationship verification for family-based benefits).
- Stated relationships (Pertinent to relationship verification for family-based benefits).
- Biographical data (Pertinent to multiple benefit and action determinations).
- Educational and vocational attainment (Pertinent to employment based benefits).
- Professional and business involvement and associations (Pertinent to employment based benefits).
- Travel information (Pertinent to multiple benefit and action determinations).
- Corporate, school and company information—many utilize social media pages rather than commercial websites (Pertinent to multiple benefit and action determinations).
- Resume postings (Pertinent to multiple benefit and action determinations).
- Blog and "Twitter" entries contrary to information submitted by the applicant. (Pertinent to multiple benefit and action determinations).
- Location information and street-views of specific addresses: May suggest an address is not a business/industry, not a residence, not a school, not a law office, not a place of worship, or not industrial, etc. (Pertinent to multiple benefit and action determinations).
- An organization's stated purposes and activities (Pertinent to terrorist and/or other inadmissibility grounds in multiple benefit and action determinations).
- An organization'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 other inadmissibility grounds in benefit determinations

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);

[9] In accordance with the September 25, 2008 Memorandum of Agreement between USCIS and ICE on the Investigation of Immigration Benefit Fraud.

- Immigration and Nationality Act of 1952, Pub. L. No. 82-414, §§ 103 and 287(a)(1) and (b), 66 Stat. 163, as amended, (8 U.S.C. § § 1103, and 1357 (a)(1) and (b);
- DHS Delegation No. 0150.1, Delegation of Authority to the Director of U.S. Citizenship and Immigration Services;
- DHS Delegation No. 15002, Delegation to the Director of U.S. Citizenship and Immigration Services to Conduct Certain Law Enforcement Activities;
- DHS Directive 110-01, Privacy Policy for Operational Use of Social Media;
- DHS Instruction 110-01-001, Privacy Policy for Operational Use of Social Media;
- USCIS Acting Director re-delegation of authority under DHS Delegation 15002 to Fraud Detection and National Security and Office of Security and Integrity, dated March 28, 2017, entitled, "Delegation of Authority to Conduct Certain Law Enforcement Activities Including, But Not Limited to, Accessing the Internet and Publicly Available Social Media Content Using a Fictitious Account or Identity;
- USCIS MD 140-001, "Handling Sensitive and Non-Sensitive Personally Identifiable Information";
- DHS Sensitive Systems Policy Directive 4300A;
- DHS Directive 047-01 "Privacy Policy and Compliance";
- DHS Instruction 047-01-001, "Privacy Policy and Compliance";
- E-Government Act of 2002, as amended, 44 U.S.C. § 101, et seq., Pub. L. No. 107-347;
- Federal Information Security Management Act of 2002 (FISMA), Title III, E-Government Act of 2002, 44 U.S.C. § 3541, et seq., Pub. L. No. 107-347; and
- Privacy Act of 1974, as amended, 5 U.S.C. § 552a, Pub. L. No. 93-579.

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 attached Rules of Behavior (RoB) for FDNS**

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;

No. Pursuant to DHS Delegation 15002, and USCIS re-delegation of DHS Delegation 15002, dated March 28, 2017, properly trained and authorized officers or employees of USCIS within or officially detailed to FDNS may access the internet and publicly available social media using a fictitious account or identity. The use of a fictitious account or identity may only be used involving matters under the jurisdiction of FDNS to protect the national security and public safety with supervisory approval. This may include allegations of articulated and/or actionable fraud concerns.

A screen name that includes an officer's name or 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; or
- Alerting an individual to the fact that they are being scrutinized by DHS. While de-confliction with law enforcement agencies is always undertaken by USCIS to avoid interference with law enforcement investigations,[10] USCIS may be the first USG entity to identify information that suggests an individual may be engaged in fraudulent or criminal behavior or a risk to national security and/or public safety.

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:

[10]In accordance with the September 25, 2008 *Memorandum of Agreement between USCIS and ICE on the Investigation of Immigration Benefit Fraud.*

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.

The Users must also complete any required trainings by the agency, in conjunction with the privacy training for operational use of social media. FDNS Officers who are authorized to access the Internet and publicly available social media content using a fictitious account or identity must be properly trained pursuant to DHS Delegation 15002.

☒ 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: 9/24/2018

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

DESIGNATION

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

PIA: Update to DHS/USCIS/PIA-013-01 Fraud Detection and National Security Directorate (FDNS); DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS)

SORN: DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, September 18, 2017, 82 FR 43556; DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) August 8, 2012, 77 FR 4741

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*.

☒ Pursuant to DHS Delegation 15002, and USCIS re-delegation of DHS Delegation 15002, dated March 28, 2017, properly trained and authorized officers or employees of USCIS within or officially detailed to FDNS may access the internet and publicly available social media using a fictitious account or identity. The use of a fictitious account or identity may only be used involving matters under the jurisdiction of FDNS to protect the national security and public safety with supervisory approval. This may include allegations of articulated and/or actionable fraud concerns.

☐ 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:

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

Please list applicable SORN here: DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, September 18, 2017, 82 FR

43556; DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) August 8, 2012, 77 FR 4741

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.

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

☐ A SORN is required:

☐ New.

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

DHS PRIVACY OFFICE COMMENTS

USCIS is submitting this SMOUT to discuss the request for access to social media for in certain instances when there are national security, public safety, or articulated and actionable fraud concerns with an application and an overt research would compromise the integrity of an investigation. In those certain instances, FDNS may use fictitious accounts or identities to review the applicant's social media content that is publicly available to all users of the social media platform.

USCIS FDNS uses social media identifiers to conduct screening and vetting checks of applicants from publicly available information on social media. Under no circumstance will DHS/USCIS violate any social media privacy settings, or directly engage in dialogue with the social media account holder. FDNS IOs may not provide false or misleading information about their identity to applicants, petitioners, or anybody else under investigation.

FDNS IOs must have approval from their supervisor not to use their official title or agency affiliation, and to use fictitious names and accounts to access social media sites. The FDNS IO names and associated fictitious account information are tracked and maintained by the FDNS IO's supervisor or manger. Cases involving use of fictitious accounts will be documented in FDNS-DS; and will be subject to routine audits by FDNS or USCIS leadership, the USCIS Office of Privacy, or the Office of Security and Integrity, either for routine audits or for-cause audits.

The approval process for the creation and use of fictitious accounts will be in accordance with the FDNS Implementation of DHS Delegation Number 15002 Standard Operating Procedures, which outlines the approval process for the creation and use of fictitious accounts, and the criteria for conducting routine and for cause audits. The SOP must be followed by FDNS supervisors and FDNS IOs.

Per the FDNS Directorate Privacy Impact Assessment (PIA) Update, and in compliance with DHS Directive 110-01, Privacy Policy for Operational Use of Social Media and Instruction 110-01-001, FDNS IOs will be permitted to access social media sites when conducting administrative investigations only after they have completed required training on the use of social media and signed the "Rules of Behavior" (RoB). FDNS IOs will then complete refresher training and sign the annually.

SORN coverage for collection, maintenance, and sharing of information by FDNS, including information obtained through social media sites is covered by DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), which covers information stored in FDNS-DS, the primary case management system for FDNS records.

SORN coverage for information that is used in an investigation, printed and saved in the applicant's Alien file is covered by DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, which covers the official record of an individual's immigration applications, petitions, and requests, as well as enforcement transactions as he or she passes through the U.S. immigration process.