



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 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](#)); 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.



For Official Use Only

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: 7/29/2019

Name of Component: U.S. Citizenship and Immigration Services, Fraud Detection and National Security Directorate (FDNS)

Contact Information: (b)(6)

Counsel² Contact Information:

Molly M. Groom, Deputy Chief Counsel USCIS (b)(6)

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.



For Official Use Only

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 U.S. Citizenship and Immigration Services (USCIS) Fraud Detection and National Security (FDNS) leads agency efforts to combat fraud, detect national security and public safety threats, and maximize law enforcement and Intelligence Community partnerships. An integral part of USCIS's delegated authority to administer the immigration laws is to conduct background, identity, and security checks on immigration requests filed with the agency. When potential fraud, public safety, or national security concerns are identified, these may be referred to FDNS for further checks or for administrative investigation. FDNS uses a variety of sources when investigating potential fraud leads or cases with national security and public safety implications, one of which is open source or publicly available web-based resources, to include accessing publicly available information from social media sites.³

The purpose of this SMOUT is to discuss the process for accessing social media information when identifying and removing systemic vulnerabilities in the process of the legal immigration system. This includes the use of overt research⁴ as well as fictitious accounts⁵ or identities in certain instances, when access to publicly-available information is only available to those who have a social

³ See DHS/USCIS/PIA-013-01 FDNS Directorate, available at www.dhs.gov/privacy, for a comprehensive list of sources used by FDNS.

⁴ Overt Research means collecting publicly available information from social media without logging in or otherwise interacting with individuals through social media. Overt research does not include creating identities or credentials on social media.

⁵ Use of fictitious accounts means 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) measure 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.



For Official Use Only

media account, and to protect the national security and public safety, and to combat immigration fraud or to identify systemic threats to the immigration system. USCIS will only access social media content that is publicly available to all users of the social media platform.

FDNS Immigration Officers (IOs) may view and gather information from social media sources to fulfill the USCIS mission of enhancing national security and integrity of the legal immigration system.⁶ FDNS may use fictitious accounts⁷ or identities for social media research, when necessary, in support of the following FDNS mission area:

Identifying and removing systemic vulnerabilities in the process of the legal immigration system: In order to identify opportunities for the best use of scarce resources, FDNS IOs conduct, or assist others in conducting, studies and analyses of benefit fraud and other systemic threats to the legal immigration systems. This work sometimes involves randomly selecting previously-adjudicated cases for review after adjudication, and reviewing or re-conducting parts of the security check process when there is an articulable basis for suspecting fraud or systematic threat to the U.S. immigration system.⁸ The use of open source and publicly available social media in these cases would be used to identify any such information that might have had an impact on an adjudication had it been known at the time the immigration request was adjudicated. These studies also help to identify fraud trends, to confirm effectiveness of security checks, and to validate efficacy of the adjudication process. In certain circumstances, information uncovered in a study might lead to further action in individual cases; for example, new evidence of fraud might lead to an investigation, and/or, where appropriate, revocation or rescission of the benefit. However, social media information does not form the sole basis for any denial, revocation, or rescission.

⁶ USCIS places a high priority on detecting, investigating and preventing immigration fraud. Immigration fraud poses a substantial threat to national security and public safety because it creates a vulnerability that may enable terrorists, criminal aliens and foreign nationals without lawful immigration status to gain entry to and remain in the United States.

⁷ Use of fictitious accounts means 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) measure 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.

⁸ See page 9 of the FDNS Program PIA for information on the types of information that might be collected in such cases. See DHS/USCIS/PIA-013-01 FDNS Directorate, available at www.dhs.gov/privacy.



For Official Use Only

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 identify threats relating to benefit fraud, national security and public safety, and systemic threats to legal immigration system. If derogatory information is uncovered by USCIS that may have an impact on adjudication, USCIS generally allows applicants⁹ the opportunity to explain and resolve any inconsistencies among information sources before USCIS issues an adjudicative decision.¹⁰

The social media reviews FDNS conducts includes a combination of overt research and use of fictitious accounts and identities. FDNS plans to use fictitious accounts and identities¹¹ during the course of its access and review of publicly available information on social media, when necessary, in support of the mission area outlined above. 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,¹² 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 identifying and removing systemic vulnerabilities only after they have completed required trainings on the use of social media and signed the "Rules of Behavior" (RoB). FDNS IOs will then complete refresher training and sign the RoB annually.

FDNS IOs may not provide false or misleading information about their identity to applicants, petitioners, or anybody else under investigation when actively engaging these individuals (i.e.,

⁹ As used in this document, the term applicant includes applicants, petitioners and requestors.

¹⁰ 8 CFR 103.2(b)(16)(i), requires that any derogatory information that an applicant or petitioner is unaware of and that may be used in an unfavorable decision must be provided to the applicant or petitioner in an interview, request for evidence, or notice of intent to deny. The applicant or petitioner 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).

¹¹ 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.

¹² See DHS/USCIS/PIA-013-01(a) FDNS Directorate, available at www.dhs.gov/privacy.



For Official Use Only

actively engaging means telephonic, written or email communications). However, FDNS IOs, with the approval of their supervisor, may use fictitious accounts or identities to passively review social media information, 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, when . 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 or public safety concerns, criminal or to combat fraud, or systematic treat to the U.S. immigration system, and overt research would compromise the integrity of an investigation, or pose an operational security risk to USCIS employees or DHS IT systems. 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 a study and/or 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).¹³

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

¹³ See DHS/USCIS/PIA-013(a) FDNS-DS, available at www.dhs.gov/privacy.



For Official Use Only

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
- 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,¹⁴ 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).

¹⁴ In accordance with the September 25, 2008 Memorandum of Agreement between USCIS and ICE on the Investigation of Immigration Benefit Fraud.



For Official Use Only

- 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);
 - 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, 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?**



For Official Use Only

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 includes combatting immigration fraud and identifying systemic threats to the immigration system.

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 IT systems 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



For Official Use Only

avoid interference with law enforcement investigations,¹⁵ 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:

- 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

¹⁵In accordance with the September 25, 2008 *Memorandum of Agreement between USCIS and ICE on the Investigation of Immigration Benefit Fraud.*



For Official Use Only

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:



For Official Use Only

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 08/09/2019

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

DESIGNATION

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

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

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.)

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE (LES)



For Official Use Only

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. When using a fictitious account or identity, FDNS IOs may use R2D2 but if FDNS IOs are doing overt research the 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 includes combatting immigration fraud.

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



For Official Use Only

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.



For Official Use Only

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 fraud concerns with a justifiable articulation for identifying and removing systemic vulnerabilities in the process of the legal immigration system. 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.

An example of using social media to identify and remove systemic vulnerabilities in the process of the legal immigration system is supported by FDNS developing the original Benefit Fraud Compliance Assessment studies to meet congressional reporting requirements and in response to a General Accounting Office (GAO) report (2002), which suggested that terrorists gain access to, or remain in, the United States through fraud and misrepresentation.

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE (LES)



For Official Use Only

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.

Additionally, the use of fictitious accounts or identities should not be the default and should only be used when necessary for national security or public safety reasons.

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 manager. Cases involving use of fictitious accounts will be documented in FDNS-DS or ECN; 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), 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.



For Official Use Only

On October 16th, 2019, this SMOUT was readjudicated for the following reason:

DHS Privacy's requested for USCIS OCC to provide a statement indicating that the removal of the citation will not impact USCIS authority to use fictitious accounts. The citations, INA § 294 and 8 USC § 1363a, do not apply to USCIS, and removal will not affect USCIS' authority to collect publicly available social media using fictitious accounts and identities. Section 294/1363a does not grant USCIS authority to conduct undercover investigation operations and activities; rather, the statute is a specific grant of authority to expend appropriated funds in support of an undercover investigation. USCIS does not receive and/or use appropriated monies to fund FDNS operational activities.

This response by USCIS OCC was coordinated with the OCC Front Office.