Exhibit C

FOR OFFICIAL USE ONLY

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

APR 0 1 2016

INFORMATION

MEMORANDUM FOR THE SECRETARY

THROUGH: Alejandro Mayorkas
Deputy Secretary

FROM: Francis X. Taylor
Under Secretary for Intelligence and Analysis

León Rodríguez
Director, U.S. Citizenship and Immigration Services

SUBJECT: **U.S. Citizenship and Immigration Services Refugee Social Media Vetting Expansion**

Purpose: To update you on U.S. Citizenship and Immigration Services' (USCIS) efforts to expand social media vetting of refugees.

Summary: On February 11, 2016, you directed the further expansion of social media use at DHS consistent with the law and appropriately protecting civil rights, civil liberties, and privacy. To that end, on December 15, 2015, you and the Deputy Secretary asked the Under Secretary for Intelligence and Analysis, Frank Taylor, to lead a Social Media Task Force to review the Department's current use of social media and identify options to optimize its use across the Department.

The Task Force determined that the first priority, and an immediate operational imperative, was to expand USCIS' ability to use social media to screen and vet applicants for immigration benefits by building upon existing capabilities that USCIS has piloted and deployed since 2014. In December 2015, USCIS and the Science and Technology Directorate (S&T) initiated additional pilots to screen K-1 Adjustment applicants and certain Iraqi and Syrian refugees. In addition to the pilots, USCIS also operationalized manual Facebook checks for the enhanced vetting process for Syrian refugees.

refugees using a manual review of an applicant's social media usage, leveraging tools to assist with automation, tradecraft and reviewing techniques learned during recent pilots with S&T. Importantly, during each of these phases, USCIS will maintain an ongoing dialogue with I&A and the Task Force to assess additional tools, to support semi-automated searches, with the objective of implementing such tools as part of the process employed by the Social Media Center of Excellence, located at the Customs and Border Protection (CBP), National Targeting Center (NTC) launching in August 2016. USCIS will also continue to partner with the Intelligence Community to hone and enhance the agency's use of social media screening.

This package includes the detailed USCIS Concept of Operations (CONOPS) for expanding Social Media Reviews of Refugees (ATCH 1), a second CONOPS, in partnership with the Department of State (DOS), to elicit social media information over a one week period from the refugee population in Turkey (ATCH 1, Appendix A), the evaluation of the refugee social media review pilot (ATCH 1, Appendix B), and social media guidance for adjudicators (ATCH 1, Appendix C).

Attachments:

1. USCIS Social Media Review of Refugees Concept of Operations
2. USCIS-DOS Elicitation Concept of Operations
3. USCIS Refugee Social Media Review Pilot Evaluation
4. USCIS Social Media Review Guidance for Adjudicators

cc: DHS Social Media Task Force

Total Number of Documents

Total Number of Matches (b)(7)(e)

Total Number of Unread By Filter (b)(7)(e)

Document Type

Language

(b)(7)(e)

Identified accounts (Y/N/Maybe)

Yes	145
No	2350
Maybe	4

Derogatory Found (Y/N/Maybe)

Yes	17
No	2474
Maybe	8

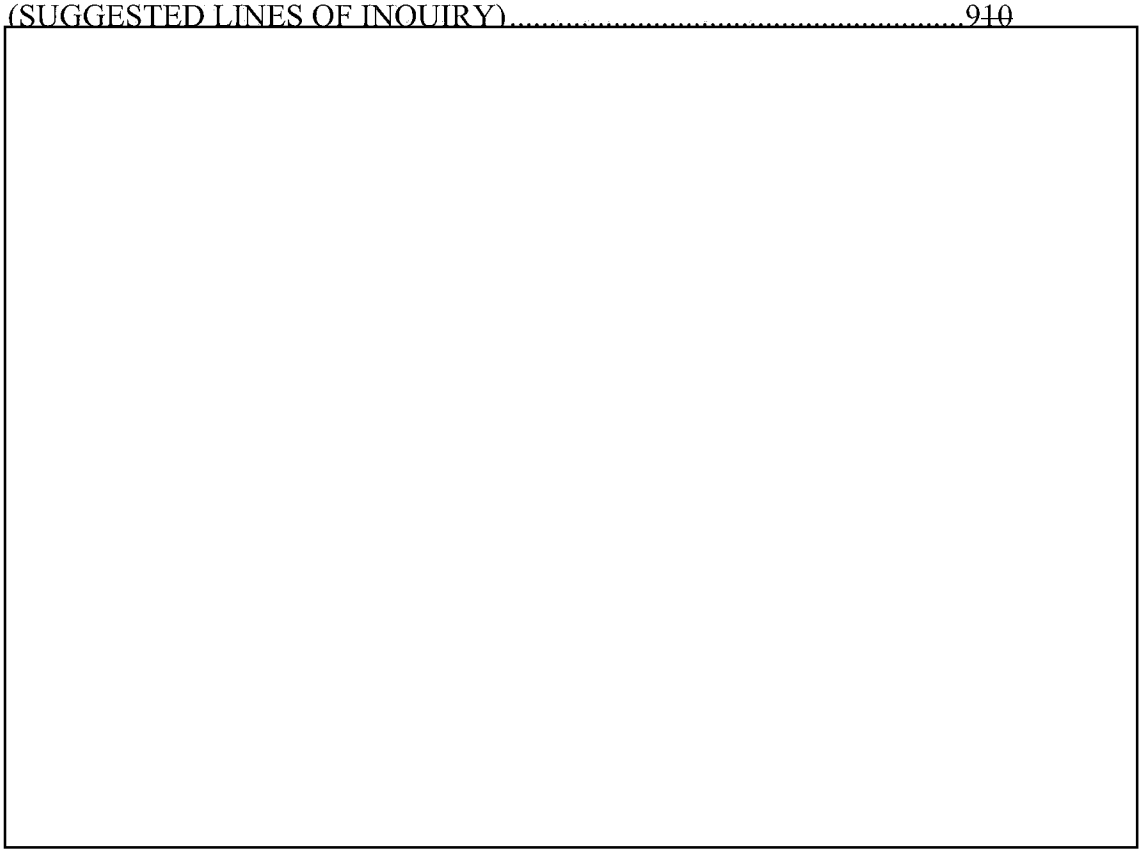
U.S Citizenship and
Immigration Services
Field Operations Directorate

GUIDANCE FOR USE OF SOCIAL MEDIA IN FIELD OPERATIONS DIRECTORATE ADJUDICATIONS

DELIBERATE, PRE-DECISIONAL DOCUMENT – DO NOT DISTRIBUTE

TABLE OF CONTENTS

(b)(7)(e)



I. PURPOSE

The purpose of this guidance is to provide adjudicating officers an understanding of how to consider and apply the results of social media checks during interviews and adjudications.

This guidance does not supersede any other guidance. Immigration Services Officers (ISOs) must obey all other adjudication policies and procedures.

II. BACKGROUND

In late 2015, USCIS began developing the Social Media Pilot Plan (SMPP), now known as the Social Media Limited Implementation Plan (SMLIP). The SMLIP was intended to explore the operational requirements, process, and functionality for using social media during the course of USCIS's work and to identify and examine potential benefits, limitations, associated costs, challenges, and risks associated with that use. Of particular relevance to FOD, social media information may help Fraud Detection and National Security Immigration Officers (FDNS IOs) and ISOs identify information that is material to benefit adjudication and potentially derogatory information.

III. FDNS PROVIDES SOCIAL MEDIA RESULTS

In general, FDNS will provide social media results as a result of an ISO's Referral to FDNS following an initial interview with the applicant. However, FDNS may also perform social media research if the case merits further research before the interview (for example, if the case is linked to a System Generated Notification in the Fraud Detection and National Security Data System).

Social media findings by FDNS IOs will be included in a Statement of Finding (SOF), Referral to ICE (RTI), or Background Check and Adjudicative Assessment (BCAA). FDNS will clearly identify how they found any indicators of potentially derogatory information on social media linked to an individual[1], will include screenshots of the potentially derogatory social media findings as a separate FDNS-DS attachment, a general description of the social media account and how it is used, and a thorough analysis of why the information is potentially derogatory. In addition, the FDNS IO will explain why the potentially derogatory information may be material and why they believe

[1] To simplify the document, applicant herein refers to an applicant, petitioner, beneficiary, or requestor.

the social media profile belongs, or does not belong, to the person in question. An ISO should ask FDNS to provide more information if they believe FDNS has not met these requirements.

The ISO will review the potentially derogatory social media information to determine if it is material to the adjudication, to develop relevant lines of questioning, and to incorporate these findings in the adjudicative process, as appropriate. Examples of relevant lines of questioning are contained as an appendix to this document.

IV. POTENTIALLY DEROGATORY INFORMATION

Potentially derogatory social media results may negatively impact admissibility or removability (such as terrorism-related and national security grounds), other eligibility factors (such as validity of claimed relationships, memberships in organizations, or criminal issues), or credibility. Due to the nature of social media, it may be difficult to conclusively determine the intent behind certain aspects of social media activity. It may be difficult to definitively attribute the activity to the applicant, determine the intent of certain activity, and to understand the activity in context (due to dialect, historical or religious connotations, slang, jargon, sarcasm, sentiment, symbolism, ambiguity, etc…).

Additionally, if the social media activity indicates an articulable link to a national security concern as described in INA 212(a)(3)(A), (B), or (F), the case must proceed through the Controlled Application Review and Resolution Program (CARRP) process.

Examples of Potentially Derogatory Information
Examples of potentially derogatory social media activity may include, but are not limited to:

- Evidence of engaging in terrorist activities as defined in INA 212(a)(3)(B);
- Potential support for armed groups/activity or for individuals/organizations associated with armed groups/activity, as defined in INA 212(a)(3)(B);
- Describing past/present/intended actions or affiliations which would make the applicant inadmissible under INA 212(a)(3)(B);
- Symbols relating to unlawful armed activity (photographs, flags, etc.);
- A social media user name that references violence or armed activity;
- Commentary that references violence or armed activity;
- Involvement with gangs or gang activity;
- Commentary that references criminal activity or suggests a public safety threat;
- Evidence of fraud, including marriage, employment, or other benefit fraud;
- Evidence that is inconsistent with information submitted on an application or petition; and

- Evidence of support of or active engagement in any illicit activity conducted by close family or friends.

V. CONFIRMING RESULTS RELATE TO THE APPLICANT

FDNS IOs will include analysis explaining how they discovered the social media activity, why they believe it can be attributed to the applicant, and if there is any ambiguity in the attribution. In many cases, an FDNS IO may provide the ISO social media information even if it cannot be clearly attributed to the applicant. This difficulty could be caused by similar biographic data, shared email accounts, or shared phone accounts. Listed below are different scenarios that officers may encounter when reviewing social media vetting results.

Social Media Account May Not Be Attributable to the Applicant
In cases where there is uncertainty that the social media account belongs to the applicant, the ISO must determine if the potentially derogatory information is relevant to the adjudication. If the information is not relevant to the adjudication, then further attribution is not required. If the information appears relevant, then the ISO must establish if the social media activity can be attributed to the applicant. This can be established by assessing how the account was initially linked to the applicant (email, phone number, name, etc.) and using related lines of questioning to determine if the account belongs to the applicant.

If the applicant credibly testifies that the social media activity is attributable to a different individual, then the officer should explore that individual and their relationship to the applicant. Concerns related to the applicant's relationship with that individual should be further explored. If the individual responsible for the social media activity raises national security concerns, the extent of the applicant's relationship to the individual with national security concerns should be explored, and the applicant's own activities and attitudes should also be assessed as they relate to those of the other individual. Officers should further assess any terrorism-related inadmissibility grounds (TRIG) or national security concerns that arise through the applicant's relationship to the individual and follow standard procedures for addressing such issues.

See Appendix A for suggested lines of questioning in cases where attribution is at question.

Social Media Account Attributable to the Applicant
If the FDNS IO determines that the social media activity is attributable to the applicant, the ISO should review the activity and verify the attribution.

The ISO must first determine if the potentially derogatory information is relevant to the adjudication. If the information is not relevant, there is no need for further analysis. If it is relevant, the officer should follow appropriate lines of inquiry to assess the derogatory information and its effect on the applicant's eligibility, assess potential TRIG and national security concerns, and follow standard CARRP, TRIG, and Public Safety procedures for addressing such issues that may arise.

During an interview, the officer should follow appropriate lines of inquiry to further verify that the social media account with potentially derogatory information belongs to the applicant and to discover if any other individual has access to, or uses, the same account. If the applicant credibly denies responsibility for the potentially derogatory information, attempt to identify the responsible party and the party's relationship to the applicant. Concerns related to the applicant's relationship with the responsible party should be explored, as previously outlined.

See Appendix A for suggested lines of questioning in cases where the account clearly belongs to the applicant.

VI. PRESENTING SOCIAL MEDIA INFORMATION

If an ISO intends to use the potentially derogatory information as evidence in a decision, the ISO must present the potentially derogatory information to the applicant during an interview or by issuing a Notice of Intent to Deny (NOID). The applicant must be given the opportunity to respond. The ISO must consider any response given during the interview or in response to the NOID.

An ISO may initially let the applicant know that the officer possesses information that needs clarification or may contradict information provided in testimony. If appropriate, the ISO may directly state what concerns were identified on the applicant's social media account so that the applicant has the opportunity to fully address the concern. This will allow the interviewing and reviewing officers to determine the full impact of the potentially derogatory information on the applicant's eligibility.

ISOs may not show applicants the SOF, RTI, or BCAA. They must instead show the social media information separately. Officers should use discretion in determining how to appropriately present potentially derogatory information sourced from social media, and may consult with their immediate supervisor or team leader on a case-by-case basis.

If an officer presents social media information, either by describing the information or by showing screenshots to the applicant, the officer should memorialize the interaction and

take a sworn statement. This will prove that the individual was presented with the evidence and given a chance to respond to it.

Note that the officer must never show the applicant a copy of the SOF, RTI, BCAA, or any other For Official Use Only (FOUO) document. The officer should also not disclose how USCIS obtained the social media information. However, the officer may describe the results to the applicant. For example, if social media results included a photograph of the applicant holding a weapon, then the officer could state that there is a photograph of that nature displayed on the social media outlet. If an officer chooses to show the applicant the derogatory information, the relevant screen shots must be detached from the FOUO document.

VII. IMPACT ON ADJUDICATION

Officers should consider social media results in the totality of the circumstances when coming to an adjudicative decision. Generally, social media results should not be the sole basis for a final decision but should instead be used to develop additional lines of questioning, prepare requests for evidence, and corroborate elements of the claim. Social media is to be considered in the context of the testimony, prior statements, documentation, and other material elements of the case, as well as the context in which the potentially derogatory information was shared on social media. Assessing the context of the social media findings might include weighing credible testimony that content was posted in jest, or by another user, or that a posting did not constitute sincere endorsement of a potentially derogatory activity.

A. CREDIBILITY

The officer must present an applicant with any material inconsistency or implausibility arising from the social media results that the officer intends to use in a denial. The officer must inform the applicant of the nature of the concern and give the applicant an opportunity to explain. Then the officer must weigh the explanation provided in the totality of the circumstances. If an officer finds that an applicant is not credible regarding a material element of his/her case, and the applicant cannot meet the required burden of proof, then the case should be denied.

For example, if an applicant testified that he/she had never used a weapon, however his/her social media results included photographs of the applicant firing weapons, the officer would confront the applicant with the inconsistency and allow the applicant an opportunity to explain. If the applicant were able to provide a reasonable explanation which resolved the inconsistency, then the officer could find the applicant credible. If the

applicant were unable to resolve the inconsistency with a reasonable explanation, then the case may be deniable.

B. INADMISSIBILITY

Applicant Admits Inadmissible Activities
If social media results indicate that an applicant is inadmissible or removable and the applicant admits to such activity, then the case should be adjudicated accordingly.

Applicant Denies Inadmissible Activities
If the applicant denies such activity, in addition to assessing the applicant's credibility, the officer will assess whether the applicant has met his/her burden of establishing that he/she is not subject to the inadmissibility by the heightened clearly and beyond doubt standard that applies to inadmissibilities. If the applicant cannot meet his/her burden with regards to the potential inadmissibility, the applicant may be found inadmissible and, in certain circumstances, also not credible, and the case will be denied.

(b)(7)(e)

D. OTHER GROUNDS OF INELIGIBILITY

If social media results lead the officer to any other adverse findings, for example a finding that the applicant had participated in persecution or was involved in marriage fraud, the officer must question the applicant to fully develop the ground(s) of ineligibility. Then, after considering the totality of the circumstances, the case would be adjudicated in accordance with standard procedure.

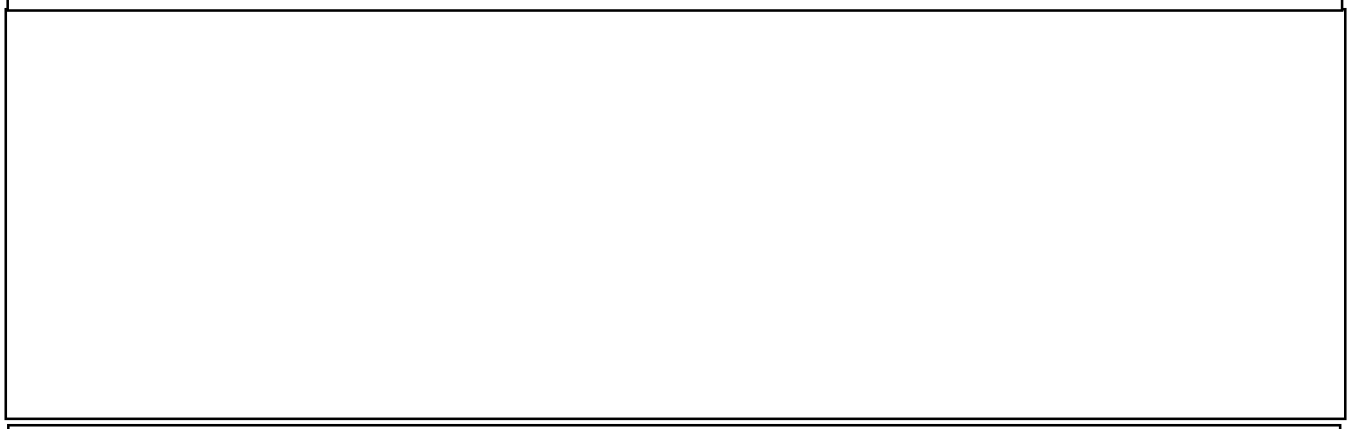
VIII. POINTS OF CONTACT

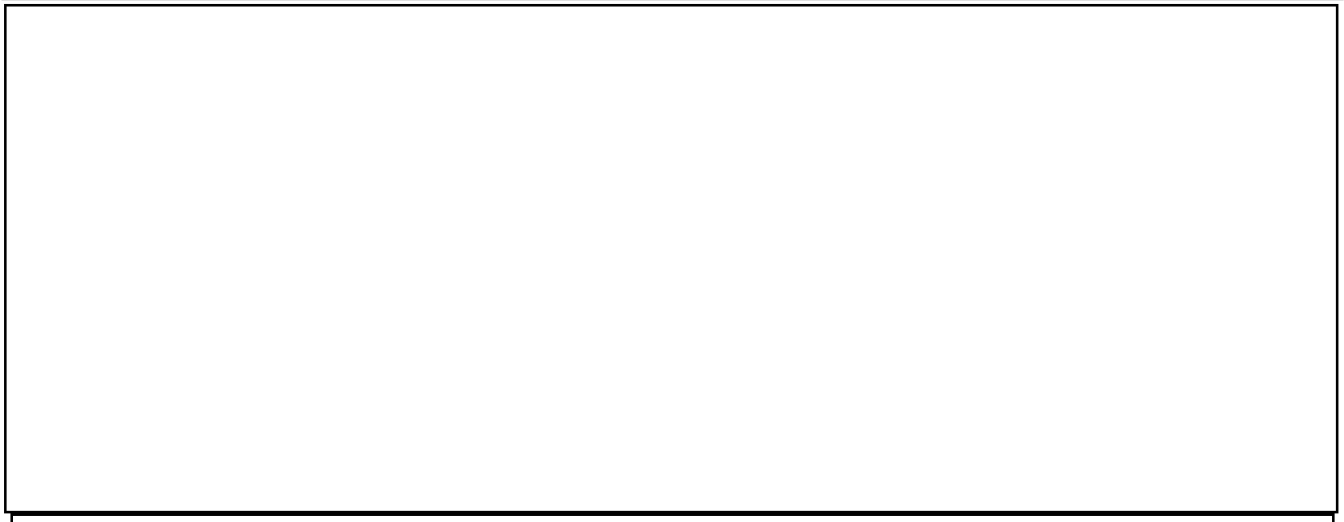
Please direct inquiries regarding FOD social media policy through proper channels to the Field Operations Directorate FDNS Operations Branch at USCISFODFDNSOps@uscis.dhs.gov.

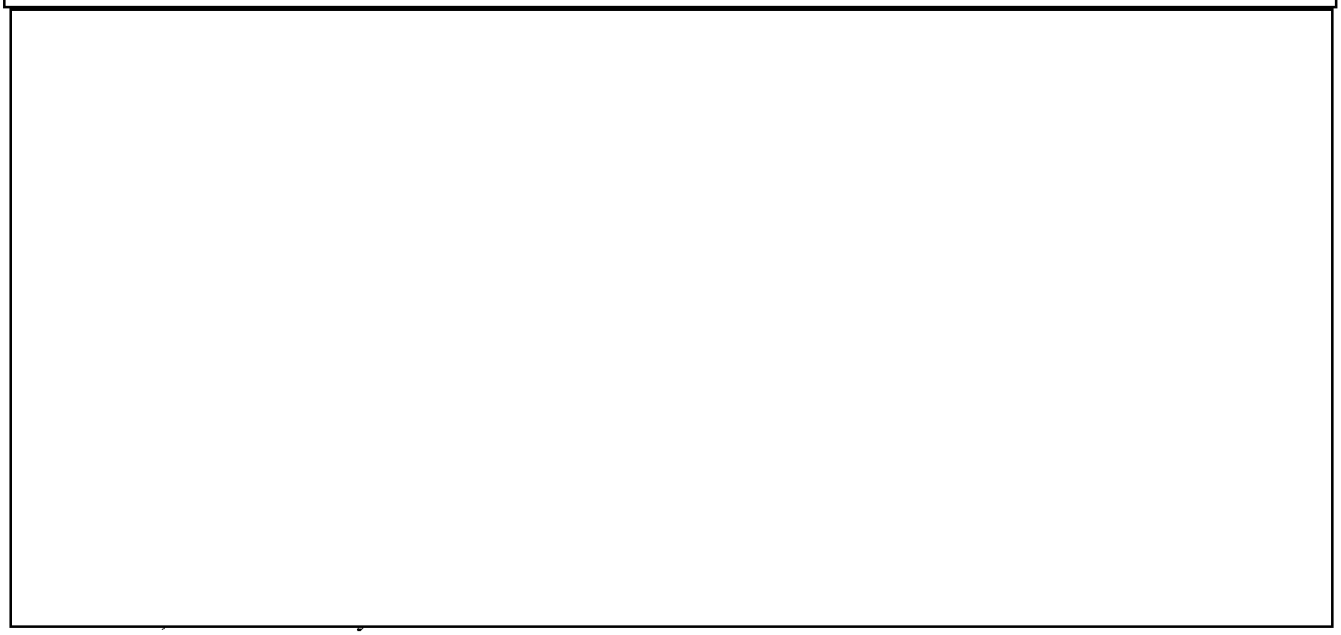
IX. APPENDIX A: ADJUDICATIVE AID FOR CASES INVOLVING SOCIAL MEDIA RESULTS (SUGGESTED LINES OF INQUIRY)

This adjudicative aid serves as a starting point for exploring potentially derogatory social media findings during an interview. Officers should keep in mind that not all potential social media scenarios are addressed in this adjudicative aid. **These lists are non-exhaustive and are designed solely to provide a framework for interviewing officers in various scenarios. Officers should not be limited to only following the suggested lines of inquiry as listed here. Officers must follow up and thoroughly probe any additional concerns not identified in this aid.** The questions do not necessarily have to be asked in any particular order, but rather should flow naturally through the course of the interview. **Additionally, note that multiple sections below may apply to the same case; it is not necessary to repeat questions which have already been asked.**

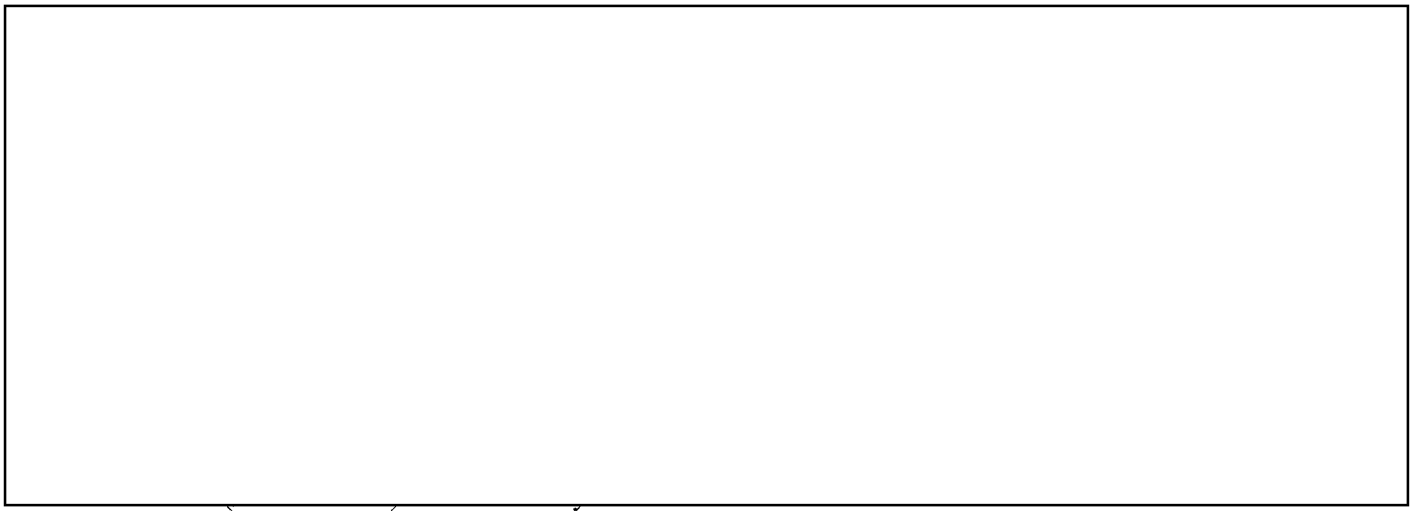
(b)(7)(e)







(b)(7)(e)



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

[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.

Homeland Security

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

Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

Homeland Security

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

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

(b)(6)

Date submitted for review: 4/30/2018

Comment [KTQ1]: Edit accepted.

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

Counsel[2] Contact Information:
Craig Symons Chief Counsel USCIS,

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

Comment [KTQ2]: Edit accepted.

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.

Homeland Security

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

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,

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

Homeland Security

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

applicants will have 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

---

[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 or general operational awareness. 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.

Homeland Security

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

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 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]

[redacted]

[redacted]

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

(b)(7)(e)

Homeland Security

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

[redacted]

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

[redacted]

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

[redacted]

Homeland Security

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

- 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, 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;

Homeland Security

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

☒ 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;

---

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

Homeland Security

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

☒ 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 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:

Homeland Security

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 SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office:

NAME of the DHS Privacy Office Reviewer: <Please enter name of reviwer.>

DESIGNATION

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

PIA: <If applicable, include PIA name and number here.>

SORN: <If applicable, include SORN name and number here.>

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.*

Homeland Security

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

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

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

b. *Email and accounts.*

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

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

c. *Public interaction.*

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

☐ Users may NOT interact with individuals online.

d. *Privacy settings.*

☐ Users may disregard privacy settings.

☐ Users must respect individual privacy settings.

e. *PII storage:*

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

Please list applicable SORN here:

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

Please list applicable SORN here:

f. *PII safeguards.*

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

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

g. *Documentation.*

Homeland Security

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

☐ 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.>

Homeland Security

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

☐ 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.>

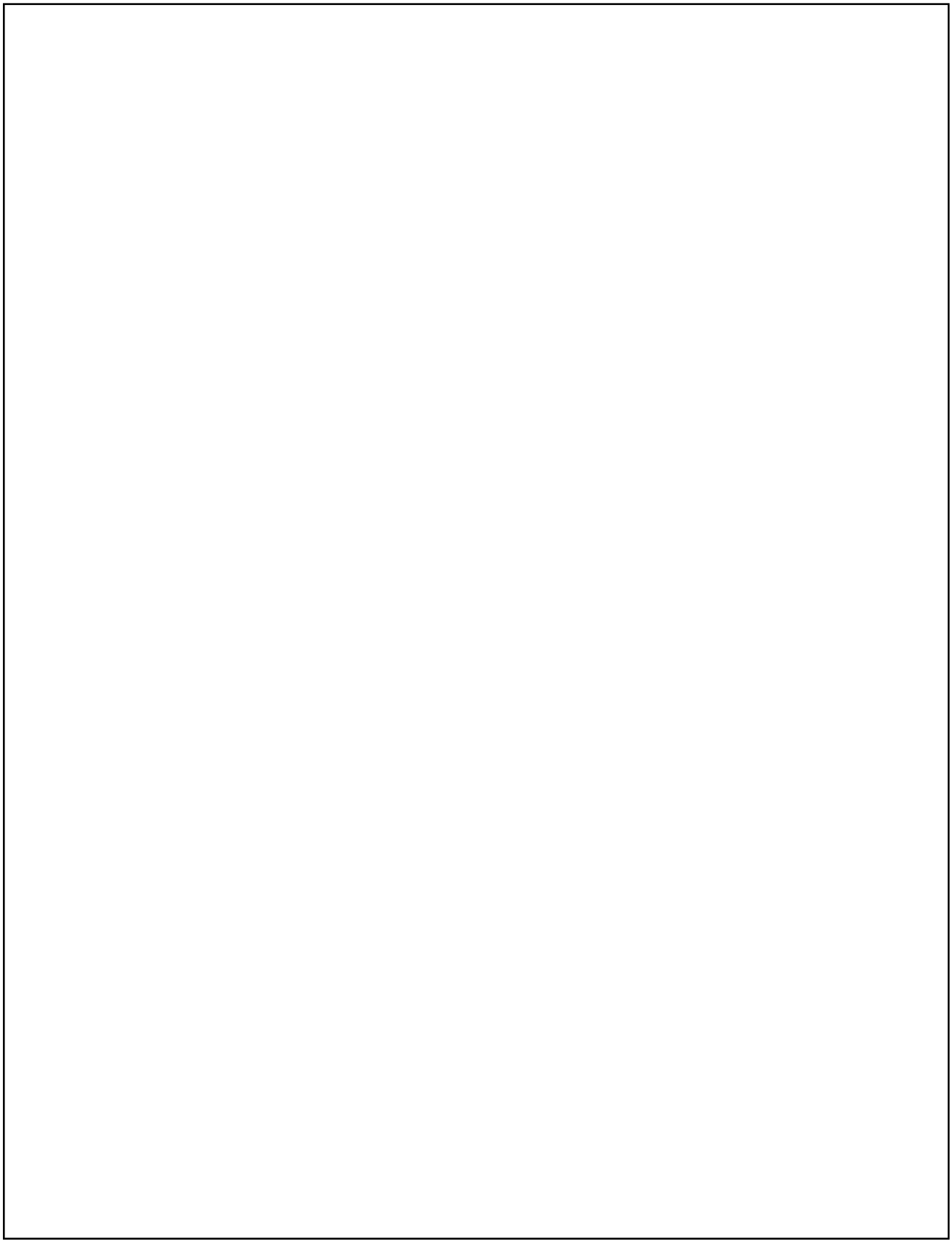
☐ A SORN is required:

☐ New.

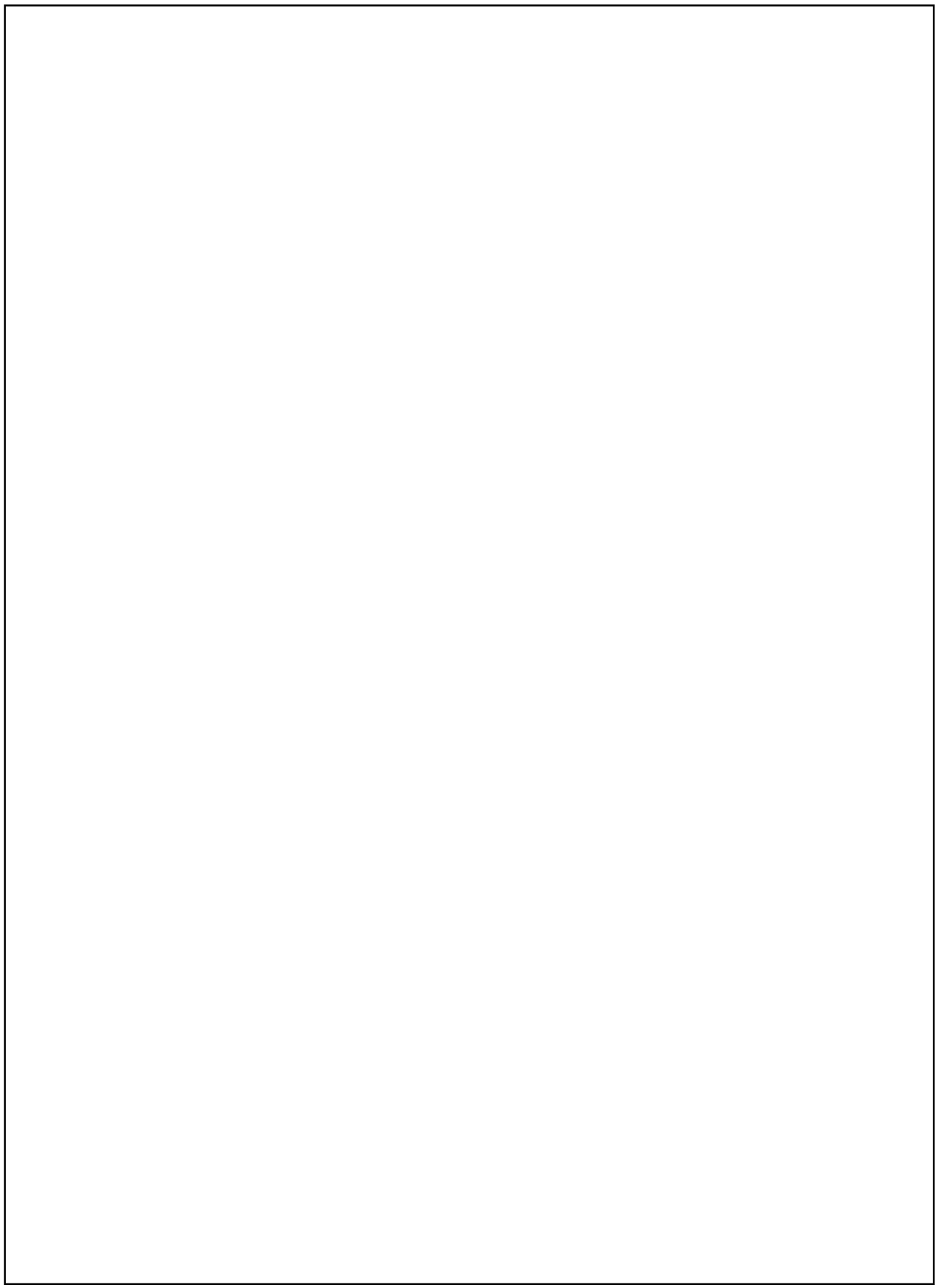
☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

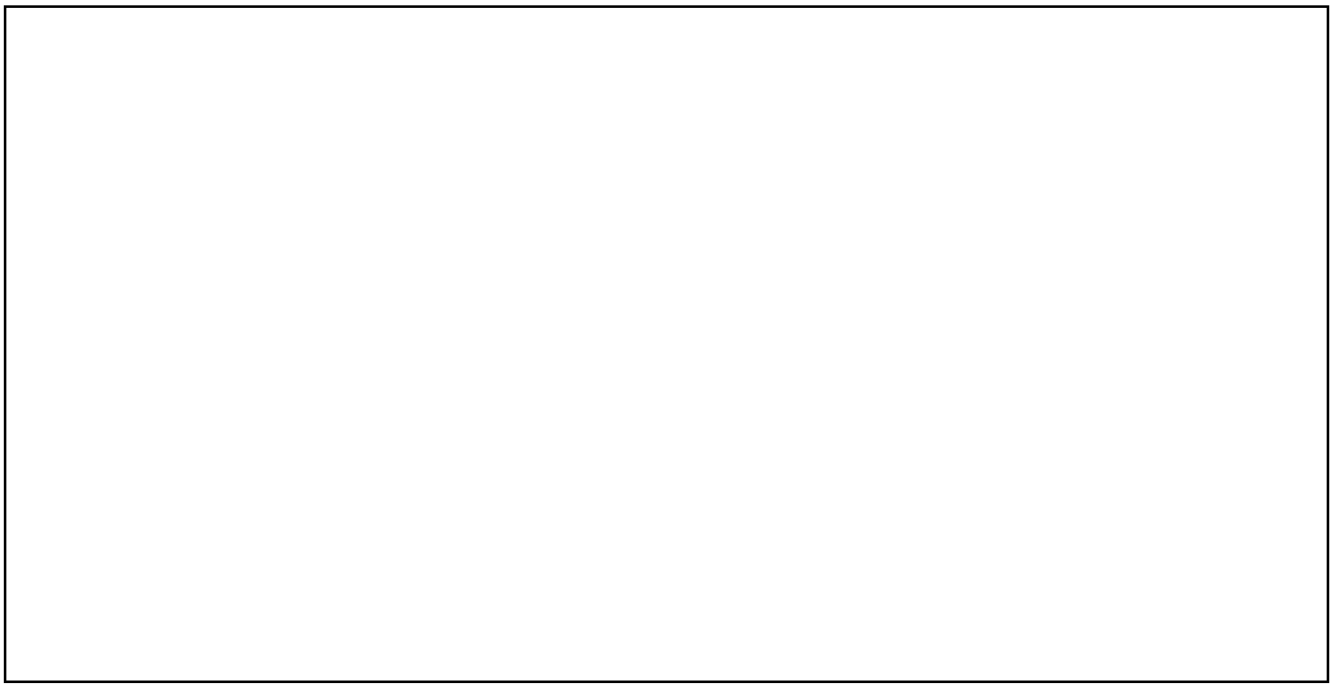
(b)(5)



(b)(5)



(b)(5)



IP – USCIS SCREENING AND VETTING

BACKGROUND

- USCIS had begun implementation of a series of initiatives as a result of Section 5 of the Executive Order (EO) 13780: Protecting the Nation from Foreign Terrorist Entry into the United States.

Interviews

- ***Expanded Interviews***
  USCIS initiated or expanded in-person interviews of applicants for immigration benefits identified as requiring additional scrutiny. Beginning in FY17, USCIS Field Operations Directorate (FOD) expanded interviews to applicants adjusting status based on an underlying K-1 fiancé(e) nonimmigrant status. FOD also began interviewing employment-based applicants adjusting status and following-to-join beneficiaries of refugee/asylee relative petitions already residing in the United States. In FY18, USCIS will further expand interviews to include individuals who consular-processed as conditional residents.
- ***Training***
  In FY16 and FY17, USCIS provided credibility and non-adversarial interview techniques training to all field offices, which will become an annual requirement starting in FY18. USCIS has also taken steps to review and implement enhanced interview training to enable officers to assess the credibility of oral testimony, determine the probative value of documentary evidence, and detect inconsistencies and other indicators of fraud or misrepresentation. Additionally, over the next few years, USCIS will implement CBP's Enhanced Communications Course (ECC) as well as national security indicator training for all interviewing officers. This training will inform interviewing officers on how to recognize and act upon national security concern indicators discovered during file review or the interview.

Screening/Vetting

- ***Continuous Immigration Vetting***
  USCIS continues development and implementation of Continuous Immigration Vetting (CIV). CIV is a collaborative effort between USCIS, Customs and Border Protection (CBP), and the National Counterterrorism Center (NCTC). In FY17, CIV

(b)(7)(e) [redacted]

Discussions regarding continuous vetting for USCIS populations against classified holdings began in FY17 and are on-going.

- ***Enhanced FDNS Review***
  Enhanced FDNS Review (EFR) is a collaborative screening process conducted by the Fraud Detection and National Security (FDNS) Directorate that includes enhanced screening of selected populations against social media and open source information, as well as [redacted] EFR is conducted for certain subsets of the refugee, refugee follow-to-join beneficiary, and asylum populations that have been assessed by the U.S. Government to present higher risk.

(b)(7)(e)

Data Collection

- ***Application Updates***
  DHS began the process to update its application forms to collect additional data elements that will be approved under three distinct generic clearances – 1) high-value biographic data elements, 2) questions requested by DOJ, and 3) social media identifiers. This additional information will be used to enhance USCIS' ability to identify potential national security threats and/or fraud among immigration applicants.
  USCIS Forms under consideration
  - N-400 Application for Naturalization
  - I-131 Application for Travel Document
  - I-192 Application for Advance Permission to Enter as a Nonimmigrant
  - I-485 Application to Register Permanent Residence or Adjust Status
  - I-589 Application for Asylum and for Withholding of Removal
  - I-751 Petition to Remove Conditions on Residence
  - I-829 Petition by Entrepreneur to Remove Conditions on Permanent Resident Status
  - I-730 Refugee/Asylee Relative Petition
  - I-590 Registration for Classification as a Refugee

Shirk, Georgette L

From: Hinds, Ian G
Sent: Wednesday, June 22, 2016 5:02 PM
To: Gaffin, Elizabeth S; Forest, Laura L; Gentry, Anthony E
Subject: FW: USCIS authority to collect/use social media information relating to the exercise of First Amendment protected activities (draft)

Importance: High

See version Dea cleared below. I plan to send to Cristina in the morning.

Ian (b)(5)

Shirk, Georgette L

From: Gentry, Anthony E
Sent: Monday, April 09, 2018 8:13 AM
To: Gaffin, Elizabeth S; Quinn, Kevin T; Brown, Sara C
Subject: RE: DHS procurement of SM services in Enhanced Vetting inititative

Regarding the CDT letter…noted with interest, not much.

From: Gaffin, Elizabeth S
Sent: Monday, April 09, 2018 9:00 AM
To: Quinn, Kevin T; Brown, Sara C
Cc: Gentry, Anthony E
Subject: RE: DHS procurement of SM services in Enhanced Vetting inititative (b)(5)

[redacted]

Elizabeth Gaffin
USCIS Office of the Chief Counsel
[redacted]
(b)(6)

From: Quinn, Kevin T
Sent: Monday, April 09, 2018 8:55 AM
To: Gaffin, Elizabeth S; Brown, Sara C
Cc: Gentry, Anthony E
Subject: RE: DHS procurement of SM services in Enhanced Vetting inititative

[redacted] (b)(5)

K

Kevin T. Quinn
USCIS - Fraud Detection and National Security
Chief – Social Media Division
[redacted] (b)(6)

From: Gaffin, Elizabeth S
Sent: Monday, April 09, 2018 8:53 AM
To: Quinn, Kevin T; Brown, Sara C
Cc: Gentry, Anthony E
Subject: RE: DHS procurement of SM services in Enhanced Vetting inititative

From CDT's letter
In July 2017, DHS held an industry day to pursue a contract to automate the current manual process of screening applicants for entry to the United States and immigration benefits as well as the process of creating deportation leads.2 In February 2018, DHS announced that it is moving forward with this contract following a closed procurement process.3 The contractor would be responsible for "exploit[ing]" information from sources such as social media websites, blogs, conferences, and academic websites.4 The contractor would be required to use automated processes to generate 10,000 investigative leads annually, to evaluate applicants' "probability of becoming a positively contributing member of society as well as their ability to contribute to the national interests," and to "assess whether an applicant intends to commit criminal or terrorist acts after entering the United States."5

Elizabeth Gaffin
USCIS Office of the Chief Counsel
[redacted] (b)(6)

From: Quinn, Kevin T
Sent: Monday, April 09, 2018 8:39 AM
To: Gaffin, Elizabeth S; Brown, Sara C
Cc: Gentry, Anthony E
Subject: RE: DHS procurement of SM services in Enhanced Vetting inititative

(b)(5) (b)(6)
[redacted]

K

Kevin T. Quinn
USCIS - Fraud Detection and National Security
Chief – Social Media Division
[redacted] (b)(6)

From: Gaffin, Elizabeth S (b)(6)
Sent: Monday, April 9, 2018 8:24 AM
To: Brown, Sara C [redacted] uinn, Kevin T <[redacted]
Cc: Gentry, Anthony E <[redacted]
Subject: DHS procurement of SM services in Enhanced Vetting inititative

https://cdt.org/insight/weighing-in-on-the-dhs-visa-lifecycle-vetting-initiative/

You are probably already aware of this

Elizabeth Gaffin
USCIS Office of the Chief Counsel
[redacted]

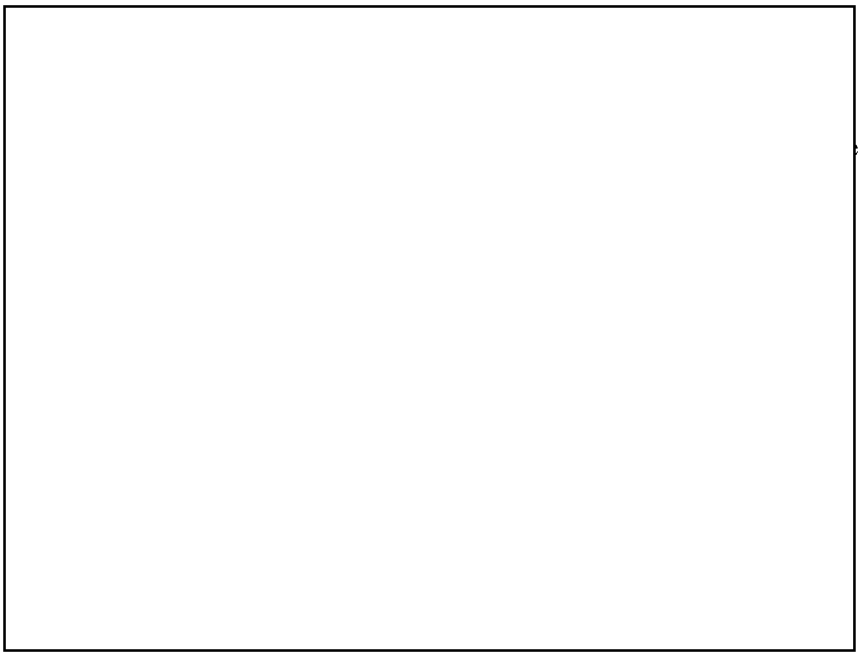
(b)(6)

U.S Citizenship and
Immigration Services
Field Operations Directorate

GUIDANCE FOR USE OF SOCIAL MEDIA IN FIELD OPERATIONS DIRECTORATE ADJUDICATIONS

TABLE OF CONTENTS

(b)(5)



I. PURPOSE

(b)(5)

The purpose of this guidance is to provide adjudicating officers an understanding of how to consider and apply the results of social media checks during interviews and adjudications.

(b)(7)(e)

This guidance does not supersede any other guidance. Immigration Services Officers (ISOs) must obey all other adjudication policies and procedures.

II. BACKGROUND

In late 2015, USCIS implemented the Social Media Pilot Project (SMPP), now known as the Social Media Limited Implementation Project (SMLIP) to provide a structured process for designated USCIS participants to test:

- The operational requirements, process, and functionality for using social media during the course of USCIS's work; and
- To identify and examine potential benefits, limitations, associated costs, challenges, and risks associated with that use. Of particular relevance to FOD, social media information may help Fraud Detection and National Security Immigration Officers (FDNS IOs) and ISOs identify information that is material to benefit adjudication and potentially derogatory.

III. FDNS PROVIDES SOCIAL MEDIA RESULTS

Social media findings by FDNS IOs are included in a Statement of Finding (SOF), Referral to ICE (RTI), or Background Check and Adjudicative Assessment (BCAA). FDNS will clearly identify how they found any indicators of potentially derogatory information on social media linked to an applicant, they will include screenshots of the potentially derogatory social media findings as a separate FDNS-DS attachment, a general description of the social media account and how it is used, and a thorough analysis of why the information is potentially derogatory. In addition, the FDNS IO will explain why the potentially derogatory information may be material and why they believe

the social media profile belongs to the person in question. An ISO should ask FDNS to provide more information if they believe FDNS has not met these requirements.

The ISO will review the potentially derogatory social media information to determine if it is material to the adjudication, to develop relevant lines of questioning, and to incorporate these findings in the adjudicative process, as appropriate. Examples of relevant lines of questioning are contained as an appendix to this document.

IV. POTENTIALLY DEROGATORY INFORMATION

Potentially derogatory social media results may negatively impact admissibility or removability (such as terrorism related and national security grounds), other eligibility factors (such as validity of claimed relationships, memberships in organizations, or criminal issues) or credibility. Due to the nature of social media, it may be difficult to conclusively determine the intent behind certain aspects of social media activity. It may be difficult to definitively attribute the activity to the applicant, determine the intent of certain activity, and to understand the activity in context (due to dialect, historical or religious connotations, slang, jargon, sarcasm, sentiment, symbolism, ambiguity, etc…).

Additionally, if the social media activity indicates an articulable link to a national security concern as described in INA 212(a)(3)(A), (B), or (F), the case must proceed through the Controlled Application Review and Resolution Program (CARRP) process.

Examples of Potentially Derogatory Information

Examples of potentially derogatory social media activity may include, but are not limited to:

- Evidence of engaging in terrorist activities as defined in INA 212(a)(3)(B);
- Potential support for armed groups/activity or for individuals/organizations associated with armed groups/activity, as defined in INA 212(a)(3)(B);
- Describing past/present/intended actions or affiliations which would make the applicant inadmissible under INA 212(a)(3)(B);
- Symbols relating to unlawful armed activity (photographs, flags, etc.);
- A social media user name that references violence or armed activity;
- Commentary that references violence or armed activity;
- Involvement with gangs or gang activity;
- Commentary that references criminal activity or suggests a public safety threat;
- Evidence of fraud, including marriage frau

(b)(5) (b)(7)(e)

- Evidence that is inconsiste [redacted] with information submitted on an application or petition; and
- Evidence o[redacted] support of or active engagement in any illicit activity conducted by close family or friend[redacted]

V. CONFIRMING RESULTS RELATE TO THE APPLICANT

FDNS IOs will include analysis explaining how they discovered the social media activity, why they believe it can be attributed to the applicant, and if there is any ambiguity in the attribution. In many cases, an FDNS IO may provide the ISO social media information even if it cannot be clearly attributed to the applicant. This difficulty could be caused by similar biographic data, shared email accounts, or shared phone accounts. Listed below are different scenarios officers may encounter when reviewing social media vetting results.

Social Media Account May Not Be Attributable to the Applicant

In cases where there is uncertainty that the social media account belongs to the applicant, the ISO must ~~first~~ establish if the social media activity can be attributed to the applicant. This can be established by assessing how the account was initially linked to the applicant (email, phone number, name, etc.) and using related lines of questioning to determine if the account belongs to the applicant.

If the applicant testifies that the social media activity is attributable to a different individual, then the officer should explore that individual and their relationship to the applicant. Concerns related to the applicant's relationship with that individual should be further explored. If the individual responsible for the social media activity raises national security concerns, the extent of the applicant's relationship to the individual with national security concerns should be explored, and the applicant's own activities and attitudes should also be assessed as they relate to those of the other individual. Officers should further assess any terrorism related inadmissibility grounds (TRIG) or national security concerns that arise through the applicant's relationship to the individual and follow standard procedure for addressing such issues. The Officer should also ascertain the credibility of the applicant's claim that the activity is not attributable to them.

See Appendix A for suggested lines of questioning in cases where attribution is at question.

Social Media Account Attributable to the Applicant

If the FDNS IO determines that the social media activity is attributable to the applicant, the ISO should review the attribution and the activity. The ISO should determine how certain the attribution is and determine if the potentially derogatory information is relevant to the adjudication. During an interview, the officer should follow appropriate lines of inquiry to further verify that the social media account with potentially derogatory information belongs to the applicant and to discover if any other individual has access to, or uses, the same account. The officer should follow appropriate lines of inquiry to assess the derogatory information and its effect on the applicant's eligibility, assess potential TRIG and national security concerns, and follow standard CARRP, TRIG, and Public Safety procedures for addressing such issues that may arise.

See Appendix A for suggested lines of questioning in cases where the account clearly belongs to the applicant.

VI. PRESENTING SOCIAL MEDIA INFORMATION

If an ISO intends to use the potentially derogatory information as evidence in a decision, the ISO must present the potentially derogatory information to the applicant during the interview or by issuing a Notice of Intent to Deny (NOID). The applicant must be given the opportunity to respond. The ISO must consider any response given during the interview or in response to the NOID.

An ISO may initially let the applicant know that the officer possesses information that needs clarification or may contradict information provided in testimony. If appropriate, the ISO may directly state what concerns were identified on the applicant's social media account so that the applicant has the opportunity to fully address the concern. This will allow the interviewing and reviewing officers to determine the full impact of the potentially derogatory information on the applicant's eligibility.

ISOs may not show applicants the SOF, RTI, or BCAA. They must instead show the social media information separately. Officers should use discretion in determining how to appropriately present potentially derogatory information sourced from social media, and may consult with their immediate supervisor or team leader on a case-by-case basis.

If an officer presents social media information, either by describing the information or by showing screenshots to the applicant, the officer should memorialize the interaction and take a sworn statement. This will prove that the individual was presented with the evidence and given a chance to respond to it.

VII. IMPACT ON ADJUDICATION

Officers should consider social media results in the totality of the circumstances when coming to an adjudicative decision. Generally, social media results should not be the sole basis for a final decision but should instead be used to develop additional lines of questioning, prepare requests for evidence, and corroborate elements of the claim. Social media is to be considered in the context of the testimony, prior statements, documentation, and other material elements of the case, as well as the context in which the potentially derogatory information was shared on social media. Assessing the context of the social media findings might include weighing credible testimony that content was posted in jest, or by another user, or that a posting did not constitute sincere endorsement of a potentially derogatory activity.

A. CREDIBILITY

The officer must present an applicant any material inconsistency or implausibility arising from the social media results that the officer intends to use in a denial. The officer must inform the applicant of the nature of the concern and give the applicant an opportunity to explain. Then the officer must weigh the explanation in the totality of the circumstances. If an officer finds by a preponderance of the evidence that an applicant is not credible regarding a material element of his/her case, then the case should be denied for not meeting the burden of proof.

For example, if an applicant testified that he/she had never used a weapon, however his/her social media results included photographs of the applicant firing weapons, the officer would confront the applicant with the inconsistency and allow the applicant an opportunity to explain. If the applicant were able to provide a reasonable explanation which resolved the inconsistency, then the officer could find the applicant credible. If the applicant were unable to resolve the inconsistency with a reasonable explanation, then the case would be denied for not meeting the burden of proof.

B. INADMISSIBILITY

Applicant Admits to enaging in activity that make him inadmissibl

If social media results indicate that an applicant is inadmissible or removable and the applicant admits to such activity, then the case should be adjudicated accordingly.

Applicant Denies engaging in activity that make him ~~I~~inadmissible ~~Activities~~

If the applicant denies such activity, in addition to assessing the applicant's credibility, the officer will assess whether the applicant has met his/her burden of establishing that he/she is not subject to the inadmissibility by the heightened clearly and beyond doubt standard that applies to inadmissibilities. If the applicant cannot meet his/her burden with regards to the potential inadmissibility, the applicant may be found inadmissible and, in certain circumstances, also not credible, and the case will be denied.

C. CARRP

D. OTHER GROUNDS OF INELIGIBILITY

If social media results lead the officer to any other adverse findings, for example a finding that the applicant had participated in persecution or was involved in marriage fraud, the officer must question the applicant to fully develop the ground(s) of ineligibility. Then, after considering the totality of the circumstances, the case would be adjudicated in accordance with standard procedure.

VIII. POINTS OF CONTACT

Please direct inquiries regarding FOD social media policy through proper channels to the Field Operations Directorate FDNS Operations Branch at

IX. APPENDIX A: ADJUDICATIVE AID FOR CASES INVOLVING SOCIAL MEDIA RESULTS (SUGGESTED LINES OF INQUIRY)

This adjudicative aid serves as a starting point for when exploring potentially derogatory social media findings during an interview. Officers should keep in mind that not all potential social media scenarios are addressed in this adjudicative aid. **These lists are non-exhaustive are designed solely to provide a framework for interviewing officers in various scenarios. Officers should not be limited to only following the suggested lines of inquiry as listed here. Officers must follow up and thoroughly probe any additional concerns not identified in this aid.** The questions do not necessarily have to be asked in any particular order, but rather should flow naturally through the course of the interview. **Additionally, note that multiple sections below may apply to the same case; it is not necessary to repeat questions which have already been asked.**

Note that under certain circumstances it may be appropriate to directly confront the applicant with social media results (however it is never appropriate to show the SOF document itself to an applicant), see Section VI for guidance on social media confrontations. **NOTE: USCIS personnel should only use electronic versions of this document and not produce any hard copies.**

1. **Social media results may or may not relate to applicant**

In some cases, it may be unclear if the potentially derogatory social media findings relate to the applicant or to another individual. For further details about such scenarios, refer to Social Media Guidance Section V: Confirming Results Relate to the Applicant. Useful lines of inquiry in such cases might include:

- How many phone numbers do you have? (list out)
- How many email addresses do you have? (list out)
- How many screen names do you have (list out)
- Other than you, are your phone numbers or email addresses used by anyone else?
- Do you have any social media accounts? How many? Which ones? (such as [redacted] etc.)
- Did you personally create each of those accounts? If not, who did?
- Do you use your real name on those accounts? If not, what names do you use on those accounts?
- Did you use your own email address on those accounts? If not, which email address did you use and to whom does it belong?
- Do you have access to any social media accounts that are not associated with you, such as a business account or one belonging to a friend or family member?

- Is your contact information (email address, telephone number) used on any other person, group, or organization's social media profile?
- How often do you check/update/post on your social media account?
- Does anyone else use your social media accounts? If so, who?

2. Applicant testifies that social media results relate to a person other than the applicant

- Describe your relationship with this person?
- Does this person now or did they in the past engage in (insert specific activity of concern) activity?
- How does this person have access to your social media account?
- Why would this person post this derogatory information on your social media account?

3. Applicant testifies that social media results involving armed groups relate to a person other than the applicant

- Does this person associate with or assist armed groups now? Did they associate with or assist armed groups in the past? Is this person a member of any armed group?
- To your knowledge, does this person support armed groups now or did they in the past?
- When did you last see or communicate with this person? How often do you communicate with this person?
- When do you expect to see or communicate with this person again?
- Where does this person currently reside? Where is this person at the moment?
- *If the person is in a terrorist organization:* Have you personally provided money, goods, or services to this person at any time in your life?

Formatted: Font: Bold

4. Applicant's social media activity indicates potential support for armed groups/activity or for individuals/organizations associated with armed groups/activity

- What interests do you list on your account/page?
- Who do you follow in your account?
- Do you follow any groups that use violence or weapons?
- Do you share information about violent or opposition groups?
- Do you share photos, images, articles, links, videos, or other people's postings that are related to violent or opposition activity?
- Do you use your social media account(s) to follow events relating to the conflict in your former home/village/neighborhood/city?
- Do you use your social media account(s) to comment on or discuss the various groups fighting against each other in (insert location)? If so, please describe.
- Do you support any of the groups fighting in (insert location), even ideologically? If so, which and why?

- Have you ever in your life posted any comments or images in support of the opposition movement in (insert location)? If so, please describe further.
- Have you ever in your life liked/followed/shared/linked to any protest or opposition group on your social media accounts? If so, which and why?
- Have you ever in your life liked/followed/shared/linked to any armed group on your social media accounts? If so, which and why?
- Have you ever in your life posted any comments or images supporting overthrow of the government in (insert location) or any other location through violence/armed opposition? If so, please describe further.

[redacted]

Formatted: Strikethrough

[redacted]

Formatted: Strikethrough

- Do you use your social media account to correspond with people who are using weapons to fight for a cause or movement? If so, who and why?
- Do you support (provide relevant group/activity from social media findings)?

5. Applicant's social media activity focuses on weapons or their user name or personal commentary references violence

- Have you ever handled a firearm? If yes, when and why?

[redacted]

[redacted]

- Do you own a gun or any other type of weapon?
- Do you collect firearms or any other weapons?
- Outside of mandatory military service, have you ever used [redacted] explosives ~~bomb,~~ or any other type of weapon, including for purposes of protecting yourself ~~ion~~ or others [redacted]
- Have you ever ~~in your life~~ posted any comments or images of guns, weapons, or violent activity? If so, please describe further.
- Do you support any of the groups fighting in (insert location), even ideologically? If so, which and why?
- Have you ever in your life liked/followed/shared/linked to any armed group on your social media accounts? If so, which and why?
- Have you ever in your life posted any comments or images supporting overthrow of the government in (insert location) through violence/armed opposition? If so, please describe further.

[redacted]

Comment [OCC10]: Duplicative.

- Do you use your social media account to correspond with people who are using weapons to fight for a cause or movement? If so, who and why?

6. Applicant's social media activity includes symbols relating to armed activity (photographs, pictures, flags, etc.)

- Do you share information about violent or opposition groups?
- Do you share photos, images, articles, links, videos, or other people's postings that are related to violent or opposition activity?
- Do you support any of the groups fighting in (insert location), even ideologically? If so, which and why?
- Have you ever in your life posted any comments or images in support of the opposition movement in (insert location)? If so, please describe further.

7. Applicant's social media activity includes images of or comments that suggest fraud (b)(5)

After confirming applicant's social media use and access, ask questions regarding the potentially derogatory images or comments that suggest fraudulent activity.

8. Applicant's social media activity includes images of or comments that suggest they are involved with criminal activity.

- Have you ever committed any crimes, even if you were not arrested, [redacted] anywhere in the world?
- Have you ever told anyone that you had committed a crime or offense? Why? (b)(7)(e)
- Disclose the potentially derogatory information found either by showing the applicant or describing it to the applicant. -Ask the applicant why they said or posted images of (insert action) and what they meant.

Office for Civil Rights & Civil Liberties

Protecting The First Amendment in Social Media Research

Presented to

Fraud Detection & National Security

DRAFT // FOR OFFICIAL USE ONLY

1878

First Amendment

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

What is First Amendment Protected Activity?

First Amendment Protected Activity:

- Public statements, thoughts, and opinions
- Association with other people, organizations, and informal groups
- Religious beliefs, practices, and expressions
- Media reporting and news stories

Many Types of Protected Activity in Social Media:

- Text
- Emojis
- Pictures
- Videos
- Music and lyrics
- "Likes"
- Forum posts
- Sharing, re-postin re -tweeting

1880

Reasonably Related

- Social media content must be "reasonably related" to the purpose for which you are investigating.
- Ask yourself "how is this helpful or relevant to the adjudication?"

USCIS Operational Use of Social Media MD [ ] states:

"Employees will limit collection of information related to First Amendment protected activities that have taken place in the United States or related to activities undertaken by United States Citizens abroad to the information that is reasonably related to adjudicative, investigative or incident responses matters."

1882

Individuals Protected Under MD [ ]

- All persons in the U.S.
- U.S. citizens in the U.S. and abroad

Social Media Research Must Be:

- Limited Purpose
- Tailored
- Even-Handed

Limited Purpose

- You must have a valid adjudicative, investigative, or incident response purpose before examining First Amendment protected activities.

Limited Purpose (Continued)

- EXAMPLE: You may collect social media information in an I-485 adjudication for a K visa to help determine the legitimacy of the marriage. But avoid digging too deeply on matters that don't relate to this inquiry, such as postings about the applicant's political interests or her social activities as that information is generally not reasonably related to determining the legitimacy of a marriage.

- You MUST NOT monitor an individual's soc media activity following final determination of a cas

1886

Tailored

- Your research, investigation, and collection of materials related to protected activity should be reasonably related to your purpose.

- Wholesale collection of all materials relating to political beliefs, associations, and religion for example should be avoided, unless they are directly related to the adjudication, investigation, or incident response.

(b)(5) (b)(7)(e)

Tailored

1888

Even-Handed

- Social media collection should be done without regard to an individual's viewpoint, or the fact of speaking itself, unless expressly relevant to the enforcement of a statute or regulation.

Even-Handed (continued)

- EXAMPLE: You may collect social media posts that help determine if an individual is an active member of a totalitarian party (as per INA 212(a)(3)(D)).

- You may not collect an individual's social media posts for a determination of status because they are known to be a spokesperson for a specific US political party or politician.

(b)(5) (b)(7)(e)

Social Media Challenges

How do you appropriately handle?

(b)(5) (b)(7)(e)

Knowledge Check

Is social media information on that association s[illegible]able for collection?

1892

Scenarios

Document Fraud Scenarios

1894

(b)(5) (b)(7)(e)

Document Fraud Scenario 1

Can this information be collected under the USCIS Social Media Polic Why?

(b)(5) (b)(7)(e)

Document Fraud Scenario 2

Can this information be collected under the USCIS Social Media P y? Why?

Benefit Fraud Scenarios

1897

(b)(5) (b)(7)(e)

Benefit Fraud Scenario 1

(b)(5) (b)(7)(e)

Benefit Fraud Scenario 2

(b)(5) (b)(7)(e)

Benefit Fraud Scenario 3

1900

National Security Scenarios

1901

(b)(5) (b)(7)(e)

National Security Scenario 1

National Security Scenario 2

National Security Scenario 3

(b)(5) (b)(7)(e)

National Security Scenario 4

Questions?

Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 11, 2016

MEMORANDUM FOR COMPONENT HEADS

FROM: Secretary Johnson

SUBJECT: Social Media Use

Social media can provide the Department with critical information related to the execution of our mission. The Department uses social media in a number of ways, which have expanded during my time as Secretary. Today, social media is used for over 30 different operational or investigative purposes by U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, Transportation Security Administration, Federal Emergency Management Agency, United States Coast Guard, United States Secret Service, Office of Intelligence and Analysis and other DHS components and offices.

I have directed the further expansion of social media use across the Department, consistent with the law and appropriately protecting civil rights, civil liberties, and privacy. To that end, on December 15, 2015, the Deputy Secretary and I asked the Under Secretary for Intelligence and Analysis, Frank Taylor, to lead a Task Force to review the Department's current use of social media and identify options to optimize its use across the Department.

I have reviewed and concur with the Task Force's recommendations based on the initial findings of its review.

As recommended by the Task Force, a first priority, and an immediate operational imperative, is to expand U.S. Citizenship and Immigration Services' (USCIS) ability to use social media to screen and vet applicants for immigration benefits, building upon the social media vetting capabilities USCIS has already piloted and deployed since 2014. USCIS and the Science and Technology Directorate (S&T) have since initiated further pilots to screen K-1 Visa applicants and certain Iraqi and Syrian refugees, which are ongoing. I direct USCIS, working with the Task Force, to evaluate and incorporate the lessons learned from these pilots and work on an expedited basis to build the capacity to conduct social media vetting on a more systematic basis across immigration benefit categories.

The second overarching priority recommended by the Task Force is to build on the work that has been done to date and expand social media use across all DHS Components. To achieve this, the Task Force recommended, and I hereby direct, the stand-up of a DHS Social Media Center of Excellence (COE) to set standards for social media use in relevant DHS operations while ensuring privacy, civil rights and civil liberties protections.

Specifically, the Center of Excellence will:

- Continuously identify gaps regarding the use of social media and serve to generate new policies and procedures to fill these gaps;
- Identify new social media tools in the marketplace and opportunities to apply them to DHS missions;
- Test these tools in coordination with S&T and Operational Components; and
- Develop and implement training to ensure the DHS enterprise is aware of and can leverage the latest state-of-the-art tools to keep pace with the evolving social media environment.

The Center of Excellence will be staffed by personnel from across the Department, including an individual from each of the oversight offices, who understand their Component's authorities. In addition, the Center of Excellence will be led by a Board of Governance, which will act as a steering committee and decision making body and will meet regularly to discuss Department-wide social media issues relating to operational, policy, and oversight issues.

To guide the Department's further use of social media, to include executing the two priority missions described above, the Task Force developed an Implementation Plan, attached herein.

I hereby direct Under Secretary Taylor and Department component heads to execute this Implementation Plan, and to achieve full operational capability of the Social Media Center of Excellence by August 1, 2016. I authorize the Task Force Chair and Co-Chairs to make amendments to the implementation plan, as necessary. I should be provided regular updates to ensure these actions are being implemented and to be apprised of any necessary amendments to the Implementation Plan. To be clear, the establishment of the Social Media Center of Excellence, as well as this memorandum, are not intended to preclude other appropriate and lawful uses of social media consistent with individual Components' legal authorities.

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of the Director
Washington, DC 20529

U.S. Citizenship and Immigration Services

Subject File Number

Memorandum

TO: Sarah Kendall, Associate Director, Fraud Detection and National Security
Joseph E. Langlois, Associate Director, Refugee, Asylum and International Operations

FROM: León Rodríguez
Director, U.S. Citizenship and Immigration Services

SUBJECT: Fraud Detection and National Security Use of Social Media for Refugee Processing

Summary
Pursuant to the terms of this memorandum and consistent with all Departmental policies, this memorandum serves as my authorization for certain non-bargaining FDNS staff, as described below, to augment the vetting of refugee applicants with a potential nexus to terrorism by conducting analysis of relevant social media.

Policy
Because refugees are located outside of the United States and have no legal status with respect to the United States until they are admitted as refugees at a port of entry, certain USCIS non-bargaining unit employees are permitted to access social media to conduct analysis on this population.

These USCIS employees, specifically Fraud Detection and National Security employees conducting background checks on refugee applicants with a potential nexus to terrorism, will conduct social media research on refugee applicants pursuant to the Social Media Operational Use Template and associated Rules of Behavior, approved by DHS Privacy.

Implementation
Employees who seek authorization to engage in the operational use of social media under this memo must:
a. Complete the USCIS Privacy Requirements for Operational Use of Social Media training program, and acknowledge they have read and understand the Component Rules of Behavior, on an annual basis;

b. Complete all training for the operational use of social media offered by FDNS, and acknowledge that they have read and understand the Rules of Behavior for that operational use of social media.

No employee may engage in the operational use of social media unless such use is consistent with this memo and all DHS and USCIS policies governing the operational use of social media.

Additionally, employees will limit collection of information related to First Amendment protected activities that have taken place in the United States or related to activities undertaken by United States Citizens abroad to the information that is reasonably related to adjudicative, investigative or incident responses matters.

These FDNS employees must also continue to coordinate with various U.S. Government entities currently conducting social media research to evaluate current procedures and best practices for social media research.

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**S&T Social Media Tool Pilot Evaluation**		
Component:	Science and Technology (S&T)	**Office or Program:**	HSARPA
Xacta FISMA Name (if applicable):	Click here to enter text.	**Xacta FISMA Number (if applicable):**	Click here to enter text.
Type of Project or Program:	**Pilot**	**Project or program status:**	**Pilot**
Date first developed:	**December 28, 2015**	**Pilot launch date:**	**December 29, 2015**
Date of last PTA update	Click here to enter a date.	**Pilot end date:**	**January 20, 2017**
ATO Status (if applicable)	Choose an item.	**ATO expiration date (if applicable):**	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	(b)(6)		
Office:	**HSARPA**	**Title:**	Director, DA-E
Phone:	(b)(6)	**Email:**	(b)(6)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

(b)(6) **Name:**			
Phone: (b)(6)		**Email:**	(b)(6)

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(7)(e)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Choose an item.

This PTA covers a study of the application of social media tools to [redacted] K-1 Visa applicants provided to S&T for testing from USCIS Fraud Detection and National Security (FDNS) Directorate. S&T will test leading edge commercial capabilities to search open source, publicly available social media using the biographic information provided by applicants on their K-1 applications.

The Department of Homeland Security is examining options to address the use of social media as part of background checks for immigrant populations. S&T is conducting a study to examine the performance, accuracy, security and utility of relevant tools on behalf of the Department in partnership with USCIS FDNS. **Initial phases of this effort are expedited to meet national requirements, and this PTA will be updated to reflect changes as the program progresses.**

This initial phase of the project will only cover [redacted] pre-selected K-1 visa applicants who have applied for adjustment of status to become Legal Permanent Residents (LPR) in the United States. This pilot will not conduct any searches regarding the petitioners on K-1 visa applications; K-1 visa petitioners are U.S. citizens.

USCIS FNDS Immigration Officers (IOs) will conduct the searches using the S&T tools and test environment. The results of the searches will be stored and maintained by USCIS, under their fraud detection and national security authorities. It is possible that information obtained may be operationally useful, and in that case, USCIS may act on the information to determine admissibility under the Immigration and Naturalization Act (INA). S&T may not use any information collected for operational purposes.

For the early phase of this program, S&T has entered into an agreement with Babel Street (via a CRADA), a social media analytics company and its Babel X product. The product operates in the Amazon commercial cloud and obfuscates user access (in this case, USCIS FDNS) to media sources and is accessed through a secure browser interface. Analytics associated with user investigations remain private to that user and their organization. In examining the social media marketplace, S&T has reviewed a number of tools and has determined that the capabilities represented by Babel Street are robust and state of the art. Babel X is also tool of choice in other agencies, including FBI.

The pilot is consistent with previously submitted and approved Social Media Operational Use Template (SMOUT) from USCIS FDNS, which permits USCIS FDNS IOs to use online screen names or accounts that do not indicate an official DHS affiliation, when collecting information from social media sources, as described from the 2014 approved SMOUT:

> Information from social media sources will be viewed and gathered by USCIS Fraud Detection and National Security (FDNS) officers during **background and administrative investigations** for cases involving possible fraud, national security, or public safety concerns.
>
> During the adjudication of immigration benefits, USCIS officers 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, officers will either provide the results to the referring adjudicator, who adjudicates the application or

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

petition 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. 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 information provided to USCIS by the applicant. Information from social media also enables USCIS to build lines of inquiry when requesting evidence and during in-person interviews.

As with all derogatory information uncovered by USCIS that may have an impact on adjudication, applicants will have the opportunity to explain or refute any adverse information discovered through social media research.

As noted in the 2012 FDNS Privacy Impact Assessment, 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 initial, training on use of social media and signed the "Rules of Behavior" form. FDNS IOs will then complete refresher training and sign the Rules of Behavior annually. When conducting official government business, FDNS IOs may not establish accounts on social media sites using fictitious names or information, or use personal accounts for official government business. FDNS IOs must use government-issued equipment to access social media. FDNS IOs cannot communicate with users of social media sites, and may only passively review information. 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).[1]

As noted above, USCIS FDNS IOs functioning under this Social Media Operational Use Template will never create fictitious names or use personal accounts for official government business. FDNS IOs will never directly interact with social media users. They will always use their official government email address when an account must be created to access a social media site, but they will not place their official title or agency affiliation in their screen names. A screen name that includes 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

[1] Privacy Impact Assessment for the Fraud Detection and National Security Directorate, DHS/USCIS/PIA-013(a), July 30, 2012.

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

specific personnel with their DHS employer;

* Encouraging those who would intentionally mislead officers by sharing false information;

* 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,[2] 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. USCIS FDNS IOs participating in the pilot will also agree to record their social media research and operational use of information obtained during the pilot, to include, at a minimum, the date, site(s) accessed, information collected, and how it is used. If information is used in connection with an active administrative investigation or case, the following data elements should be recorded:

- FDNS-DS CME number
- Nature of the concern (Fraud, public safety, national security, other)
- Why are you searching?
- Websites searched (Facebook, Google (incl. subsidiaries), Twitter, others)
- Search elements used (name, email address, physical address, others)
- Nature of information found
- Relevance of information to investigation or adjudication
- Time spent on research
- Notes for Headquarters
- Date accessed
- A screen shot showing the relevant information

USCIS FDNS IOs may use the Babel X tool to conduct searches, provided they use their government issued emails and identities to create accounts. S&T has not completed a SMOUT for the operational use of social media, and therefore cannot mask their identities online, nor conduct un-attributable searches.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☒ Social Media ☐ Web portal[3] (e.g., SharePoint) ☐ Contact Lists

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

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

	☐ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[4] ☒ Members of the public ☐ DHS employees/contractors (list components):USCIS, S&T ☐ Contractors working on behalf of DHS ☐ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?

For this early phase of the pilot, information regarding pending K1 Visa Applicants, the beneficiaries, and not petitioners, is being loaded into the Babel X system for use by DHS USCIS FDNS immigration officer accounts. These applicants represent pending applications for adjustment of status to Legal Permanent Resident (LPR) and were not selected by any other external criteria. Employees from Babel Street who are involved in this effort are covered by DHS Non-disclosure agreements and terms of the S&T HSARPA Cooperative Research And Development Agreement (CRADA). Information provided to Babel Street for the purposes of expediting searches will be handled in accordance with the DHS NDA and the CRADA agreement, which requires written certification of data destruction to S&T within two days of destruction of data, and no later than the end of the 30 day period of performance of the CRADA.

K1 beneficiary information, including full names, social security numbers, alien numbers (A Number), receipt numbers, phone numbers, street addresses, and email information is being used to analyze open source "broadcast" social media information streams from up to 29 social media platforms. In all cases, information is accessed in accordance with privacy policies of the underlying platform. This means that all searches will be conducted using open source material and that USCIS FDNS users must respect individuals' privacy settings and access only information that is publicly available. This is automatic, data within Babel Street is only made available to users in accordance with the privacy policy of the underlying data source.

(b)(7)(e)

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(7)(e)

USCIS has provided up to eleven immigration officers to work with S&T's configuration of Babel X. USCIS officers will rely on USCIS FDNS authorities to review pending K1 Visa applications and to explore the development of social media Concept of Operations (CONOPS). FDNS Immigration Officers have extensive experience with fraud detection and national security and are essential to the evaluation of technical capability and the relevance of data sources and technical capabilities. S&T will document the performance of Babel X as a first social media analytics capability for the pilot, its operational efficacy, and technical gaps that can be later addressed by research and development. Information related to the operational experiment will be held in the Babel X system hosted on an Amazon server. The S&T Information Systems Security Officer (ISSO) for the HSARPA Data Analytics Laboratory has conducted a preliminary assessment of the Babel X security architecture. S&T DA-E ISSO is continuing to assess the security features of the Babel X system. There is a clear boundary between the government system and Babel X at the point of query. When the pilot is terminated, data from the pilot will be destroyed, or with proper authorization may reside in accounts that are appropriately transitioned to USCIS FDNS ownership.	
4(a) Does the project, program, or system retrieve information by personal identifier?	☐ No. Please continue to next question. ☒ Yes. If yes, please list all personal identifiers used: Full Name, Social Security Number, Street Address, Phone Number, Email Address, Alien Number (A-Number)
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☐ No. ☒ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	SSNs from non-US citizens are collected by USCIS as part of the K1 Visa Application process and are used by USCIS FDNS to facilitate background checks.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	SSNs from non-US citizens are collected by USCIS as part of the K1 Visa Application process and are used by USCIS FDNS to facilitate background checks. During this pilot, S&T will use the K1 beneficiary, and not the petitioner, SSNs to conduct biographic matches of open source information on social media. If an SSN is used in the open source content of social media, it will become part of the keywords that indicate a biographic match within a social media posting that could be related to a specific K-1 applicant.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic,

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?	please answer the following question.
4(f) If header or payload data[5] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☐ No. ☒ Yes. If yes, please list: PII for pending K1 Visa beneficiaries was provided by FDNS to S&T to facilitate the initial phase of the pilot. There is no connection between the pilot system and other DHS systems.
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☐ No. ☒ Yes. If yes, please list: Information regarding pending K1 Visa applicants is provided to Babel Street for loading into the DHS immigration officer accounts for efficiency and in order to meet internal deadlines. This data will be certified as destroyed by Babel street in 2 days.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	New Please describe applicable information sharing governance in place: The DHS S&T CRADA outlines the information sharing process with Babel Street and provides strict guidance. The CRADA was signed on 24 December 2015, and modified by an addendum on 29 December 2015 to enable data sharing and impose terms of data use

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.
[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

	and retention.
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: These issues will be resolved once efficacy of the technology is determined and CONOPS are clear. ☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[6]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity: ☒ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☒ Low ☐ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:		**S&T Privacy Officer**	(b)(6)

[6] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

Date submitted to Component Privacy Office:	**December 29, 2015**
Date submitted to DHS Privacy Office:	December 29, 2015
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.* Click here to enter text.	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
PCTS Workflow Number:	**1116094**
Date approved by DHS Privacy Office:	December 29, 2015
PTA Expiration Date	March 1, 2016

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. ☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	**System covered by existing PIA** If covered by existing PIA, please list: DHS/USCIS/PIA-013(a) - Fraud Detection and

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

	National Security Directorate (FDNS)
SORN:	System covered by existing SORN If covered by existing SORN, please list: • DHS/USCIS-006 - Fraud Detection and National Security Records (FDNS) August 8, 2012, 77 FR 47411 • DHS/USCIS/ICE/CBP-001 – Alien File, Index, and National File Tracking System of Records, November 21, 2013, 78 FR 69864

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

The DHS Privacy Office (PRIV) finds that the Babel X social media pilot conducted by S&T and USCIS is a privacy sensitive information collection from members of the public. Therefore, a PIA and a SORN are required as part of this initiative.

USCIS FDNS Immigration Officers (IO) will conduct the searches using the Babel X social media analytics tool under their authorities to conduct background and administrative investigations for cases involving potential fraud, national security, or public safety concerns. As noted in the 2012 FDNS Privacy Impact Assessment, in compliance with *DHS Directive 110-01, Privacy Policy for Operational Use of Social Media and Instruction 110-01-001*, FDNS IOs are permitted to access social media sites when conducting administrative investigations only after they have completed initial, training on use of social media and signed the "Rules of Behavior" form. FDNS IOs will then complete refresher training and sign the Rules of Behavior annually. When conducting official government business, FDNS IOs may not establish accounts on social media sites using fictitious names or information, or use personal accounts for official government business. FDNS IOs must use government-issued equipment to access social media. FDNS IOs cannot communicate with users of social media sites, and may only passively review information. 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).[7] At a minimum, FDNS IOs must document the date, site(s) accessed, information collected, and how it is used. If information is used in connection with an active administrative investigation or case, the following data elements should be recorded in FDNS-DS:

- FDNS-DS CME number
- Nature of the concern (Fraud, public safety, national security, other)
- Why are you searching?
- Websites searched (Facebook, Google (incl. subsidiaries), Twitter, others)
- Search elements used (name, email address, physical address, others)
- Nature of information found
- Relevance of information to investigation or adjudication

[7] Privacy Impact Assessment for the Fraud Detection and National Security Directorate, DHS/USCIS/PIA-013(a), July 30, 2012.

Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

- Time spent on research
- Notes for Headquarters
- Date accessed
- A screen shot showing the relevant information

FDNS IOs will follow the standard Rules of Behavior provided in DHS Instruction 110-01-001 with the exception of the requirement to use screen names or identities that indicate an official DHS affiliation. With supervisor approval, FDNS IOs may use a screen name that does not indicate an official DHS affiliation when the use of a DHS affiliation would make the subject or other material witness aware of the existence of an ongoing investigation or would jeopardize investigative efforts. For auditing and accountability purposes, USCIS must maintain a list of all such employees and their associated screen names. However, FDNS IOs must use their own names and official DHS email addresses to create online accounts. **[PLEASE SEE APPENDIX FOR FDNS RULES OF BEHAVIOR TEMPLATE].**

As noted above, USCIS FDNS IOs functioning under this Social Media Operational Use Template will never create fictitious names or use personal accounts for official government business. FDNS IOs will never directly interact with social media users. **They will always use their official government email address when an account must be created to access a social media site, but they will not place their official title or agency affiliation in their screen names.**

USCIS FDNS IOs may use the Babel X tool to conduct searches, provided they use their government issued emails and identities to create accounts. **S&T has not completed a SMOUT for the operational use of social media, and therefore cannot collect personally identifiable information from social media, mask their identities online, nor conduct unattributable searches.**

The FDNS PIA provides PIA coverage for FDNS IO use of social media for administrative investigations. The FDNS PIA acknowledges that FDNS IOs may conduct searches of social media sites when conducting administrative investigations after the IO has completed annual training on the use of social media and signed rules of behavior. In the PIA, FDNS also committed to completing a policy for the use of social media prior to using social media for operational purposes.

Any information, whether or not that information is derogatory, that is collected from a social media site and used as part of an investigation is saved in the individual's A-File and electronically recorded in FDNS-DS. The A-File SORN covers the social media information placed in an individual's A-File. The A-File SORN should be updated to include publicly available information on the internet as a record source category, but this update is not required before FDNS IOs may access social media. The FDNS SORN covers information stored in FDNS-DS.

Following this test, S&T will provide a "hot wash" for representatives from OGC, PRIV, and CRCL to review the filters, test results, and all information collected. USCIS must provide certification of training and signed Rules of Behavior for FDNS IOs to the FDNS Privacy Officer within one week of this PTA.

U.S Citizenship and
Immigration Services
Refugee Affairs Division

GUIDANCE FOR USE OF SOCIAL MEDIA IN SYRIAN REFUGEE ADJUDICATIONS

TABLE OF CONTENTS

[redacted]

(b)(7)(e)

I. PURPOSE

The purpose of this guidance is to provide officers with information and tools to use the results of social media checks in the refugee adjudication process.

II. BACKGROUND

In early 2016, USCIS began implementing social media checks or searches in a few adjudication types. As a result of this effort, in January/February 2016 the Syria Enhanced Review Process was expanded to include social media checks on all Syrian cases referred to the Fraud Detection and National Security Directorate (FDNS) by the Refugee Affairs Division (RAD). In cases where FDNS enhanced review results in findings of potentially derogatory information, those results are detailed in a Refugee Case Analysis and Threat Summary (RCATS) document and provided to RAD for use in the interview and adjudication process. The RCATS document includes FDNS results of open source, classified and social media research permissible in a For Official Use Only format.

III. PRESENTATION OF SOCIAL MEDIA RESULTS

Social media findings by FDNS are included in the RCATS, in the Social Media Results section. In this section, FDNS will identify whether they found any indicator of potentially derogatory information on social media linked to an applicant, and if so, the RCATS may include screenshots of the social media findings, as well as FDNS analysis of why the information is potentially derogatory. Prior to adjudicating a Syrian refugee case, the interviewing officer is required to review the entry for that case on the Syria Case Profiles ECN, and if a case has an RCATS attached, the officer will review it to inform their lines of questioning and incorporate these findings in the adjudicative process, as appropriate. Officers must place on HQ hold all cases where FDNS has provided RAD with potentially derogatory information (including from social media results). The RAD Security Vetting and Program Integrity (SVPI) unit will review those HQ holds and make a final determination on the case. Refer to the Syria Field Resource Guide for the most recent guidance on the Syrian review process.

IV. DEROGATORY INFORMATION

Generally, derogatory information sourced from social media includes any information that could impact the applicant's eligibility for resettlement through the U.S. Refugee Admission Program (USRAP). Derogatory social media results may negatively impact an applicant's access to the USRAP, whether they meet the refugee definition (including persecutor bar), admissibility (including terrorist related and national security grounds),

firm resettlement or credibility. Due to the nature of social media, it may be difficult to conclusively determine the intent behind certain aspects of social media activity. Such challenges may include definitively attributing the activity to the applicant, determining the intent of certain activity, and considering factors such as context, sentiment, or the possibility of sarcasm or joking.

Social media activity will be considered derogatory if it negatively impacts the applicant's access, refugee claim, admissibility, firm resettlement or credibility. Additionally, if the social media activity implicates an articulable link to a national security concern as described in INA 212(a)(3)(A), (B), or (F), the case must proceed through the Controlled Application Review and Resolution Program (CARRP) process.

Examples of potentially derogatory social media activity may include, but are not limited to:

- Evidence of engaging in terrorist activities as defined in INA 212(a)(3)(B)
- Indicates potential support for armed groups/activity or for individuals/organizations associated with armed groups/activity, as defined in INA 212(a)(3)(B)
- Describing past/present/intended actions or affiliations which would make the applicant inadmissible under INA 212(a)(3)(B)
- Symbols relating to armed activity (photographs, pictures, flags, etc.)
- A social media user name that references violence or armed activity
- Commentary that references violence or armed activity

If derogatory information is identified prior to interview, SVPI will review the information prior to interview to determine if there is a force protection issue that would make the interview of the applicant inadvisable for security reasons, and if so, will inform the appropriate RAD Desk Officer and Regional Security Officer (RSO) responsible for that region.

V. CONFIRMING RESULTS RELATE TO THE APPLICANT

In the Social Media Results section of the RCATS, FDNS will include analysis of how they discovered the social media activity, how they attributed it to the applicant, and whether there is any ambiguity in the attribution. In some cases, it may not be clear that the social media activity can actually be attributed to the applicant. This could occur in cases of similar names, shared email accounts, shared phone accounts, or where profile-type photos do not appear to be of the applicant.

In cases where there is uncertainty that the social media account belongs to the applicant, the officer must first establish if the social media activity can be attributed to the applicant. This may be established by assessing how the account was initially linked to

the applicant (email, phone number, name, etc.) and using lines of questioning to determine if the account belongs to the applicant.

If the applicant testifies that the social media activity is attributable to a different individual, then the officer should explore who that individual is and that individual's relationship to the applicant. Concerns related to the applicant's relationship with that individual should be further explored. If the individual responsible for the social media activity raises national security concerns, the extent of the applicant's relationship to the individual with national security concerns should be explored, as well as the applicant's own activities and attitudes should also be assessed as they related to those of the other individual. Officers should further assess any Terrorist Related Inadmissibility Ground (TRIG) or national security concerns that arise through the applicant's relationship to the individual and follow standard procedure for addressing such issues.

See Appendix for suggested lines of questioning in cases where attribution is at question.

If the social media activity is attributable to the applicant, the officer should directly confront the applicant with the activity and provide the applicant the opportunity to explain. The officer should follow appropriate lines of inquiry to assess potential TRIG and national security concerns, and follow standard procedure for addressing such issues.

See Appendix for suggested lines of questioning in cases where the account clearly belongs to the applicant.

VI. CONFRONTING AN APPLICANT USING SOCIAL MEDIA RESULTS

An officer must address the potentially derogatory information and its impact on the applicant's eligibility by confronting the applicant and giving him/her the opportunity to respond. Officers should use discretion in determining how to appropriately confront applicants with potentially derogatory information sourced from social media, and may consult with their immediate supervisor or team leader on a case-by-case basis.

An officer may initially let the applicant know that the officer possesses information that needs clarification or may contradict information provided in testimony. If appropriate, the officer may directly state what concerns were identified on the applicant's social media account so that the applicant has the opportunity to fully address the concern. This will allow the interviewing and reviewing officers to determine the full impact of the potentially derogatory information on the applicant's eligibility. However, the officer should never show the applicant a copy of the RCATS itself or the information contained in the Social Media Results section, nor disclose how USCIS obtained the information.

VII. IMPACT ON ADJUDICATION

Officers should consider social media results in the totality of the circumstances when coming to an adjudicative decision. This includes consideration of testimony, prior statements, documentation, and other material elements of the case, as well as the context in which the potentially derogatory information was shared on social media. Assessing the context of the social media findings might include weighing credible testimony that content was posted in jest, or by another user, or that a posting did not constitute sincere endorsement of a concerning activity.

Pursuant to current policy, officers must place on HQ hold for SVPI review all cases where FDNS has provided RAD with potentially derogatory information sourced from social media. Refer to the Syria Field Resource Guide for the most recent guidance on the Syrian review process.

A. CREDIBILITY

Pursuant to standard procedure (see RAIO Credibility Lesson Plan), the officer must confront an applicant on any material inconsistency, lack of detail, or implausibility arising from the social media results. The officer must inform the applicant of the nature of the concern and give the applicant an opportunity to explain. Then the officer must weigh the explanation in the totality of the circumstances. If an officer finds an applicant not credible to a material element of his/her case, then the case should be denied per standard procedure.

For example, if an applicant testified that he/she had never used a weapon, however his/her social media results included photographs of the applicant firing weapons, the officer would confront the applicant with the inconsistency and allow the applicant an opportunity to explain. If the applicant were able to provide a reasonable explanation which resolved the inconsistency, then the officer could find the applicant credible and place the case on HQ hold for SVPI review per standard procedure. If the applicant were unable to resolve the inconsistency with a reasonable explanation, then the case would be denied based on an adverse credibility finding that was material to an inadmissibility.

B. INADMISSIBILITY

If social media results indicate that an applicant is inadmissible, e.g. images of military-type training by, potential current membership in, or evidence of material support to, a terrorist organization, and the applicant admits to such activity, then the case should be denied due to the applicable inadmissibility, per standard procedure.

If the applicant denies such activity, in addition to assessing the applicant's credibility, the officer will assess whether the applicant has met his/her burden of establishing that

he/she is not subject to the inadmissibility by the heightened clearly and beyond doubt standard that applies to inadmissibilities. If the applicant cannot meet his/her burden with
(b)(7)(e) regards to the potential inadmissibility, the applicant may be found inadmissible and, in certain circumstances, also not credible, and the case will be denied.

D. OTHER GROUNDS OF INELIGIBILITY

If social media results lead the officer to any other adverse findings, for example a finding that the applicant had participated in persecution or was firmly resettled, then the case would be denied in accordance with standard procedure.

VIII. POINTS OF CONTACT

Please direct inquiries regarding RAD social media policy to the RAD Branch Chiefs for Policy and SVPI with the appropriate Regional Operations desk in copy.

IX. APPENDIX: ADJUDICATIVE AID FOR CASES INVOLVING SOCIAL MEDIA RESULTS

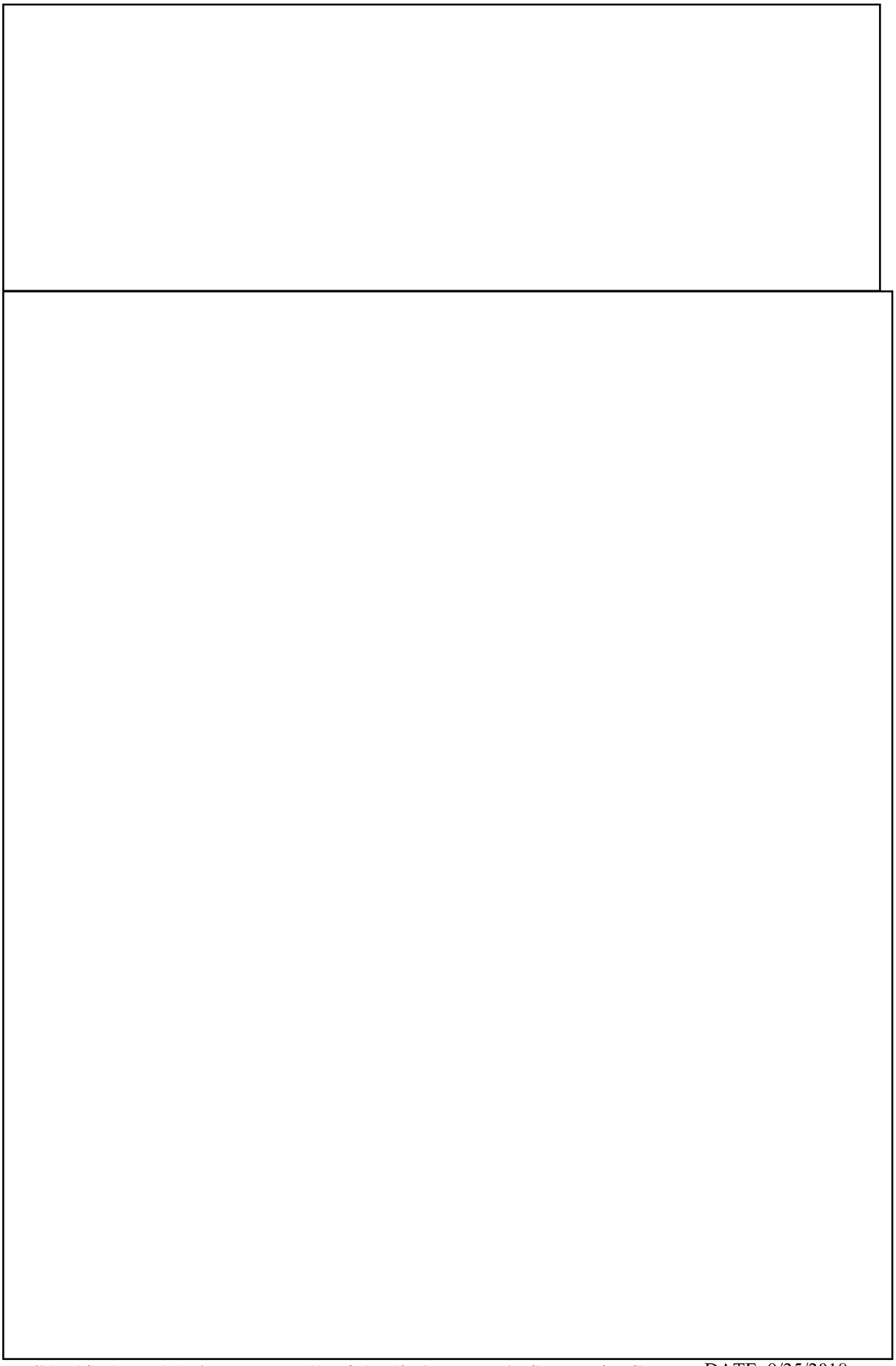
Exploration of potentially derogatory social media findings should not be limited to the suggested questions in this adjudicative aid. Any additional concerns not identified in this aid should be thoroughly probed. These questions are not exhaustive and are designed solely to provide a framework for interviewing officers in particular scenarios. They should not be asked explicitly in this order, but should flow naturally through the course of the interview. It is requested that any USCIS personnel that uses this aid not produce hard copies of this document and keeps it as an electronic copy only.

A. OBJECTIVE

This adjudicative aid is intended to assist adjudicators in the field with suggested lines of inquiry that address common types of potentially derogatory social media activity adjudicators may encounter in refugee adjudications. The questions are not required, but are rather intended to help the officer understand and elicit the information necessary to assess concerns rising from social media results.

Officers should keep in mind that not all potential social media scenarios are addressed in this adjudicative aid. Once questioned further, an applicant's testimony of the details surrounding the potentially derogatory social media activity may establish to the adjudicator's satisfaction that the concern is resolved favorably by testimony. For further detail regarding how social media findings may impact adjudicative decisions, refer to Section VII above. (b)(7)(e)

(b)(7)(e)



(b)(5) (b)(7)(e)

(b)(7)(e)

(b)(7)(e) (b)(5)