Privacy Impact Assessment Update
for the

Fraud Detection and National Security Directorate

DHS/USCIS/PIA-013-01(a)

July 26, 2019

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8030

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) is updating the Privacy Impact Assessment (PIA) for the Fraud Detection and National Security Directorate (FDNS), published on December 16, 2014. The purpose of this update is to discuss changes to the process for accessing social media information when conducting certain background, identity, and security checks.[1] Primarily, this relates to the use of fictitious accounts[2] or identities in certain instances, when access to publicly-available information is only available to those who have a social media account, and to protect the national security and public safety and to combat immigration fraud.[3] USCIS will only access social media content that is publicly available to all users of the social media platform.

Overview

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) implements immigration law and policy through the processing and adjudication of applications, petitions, and other immigration-related requests (hereinafter referred to as immigration requests).[4] USCIS's Fraud Detection and National Security Directorate (FDNS) leads agency efforts to combat fraud, detect national security and public safety threats, and maximize law enforcement and Intelligence Community partnerships. An integral part of USCIS's delegated authority to administer the immigration laws is to conduct background, identity, and security checks on immigration requests filed with the agency. When potential fraud, public safety, or national security concerns are identified, these may be referred to FDNS for further checks or for administrative investigation. FDNS uses a variety of sources when investigating potential fraud leads or cases with national security and public safety implications, one of which is open source or publicly available web-based resources, to include accessing publicly available information from social media sites.[5] DHS defines social media as the "sphere of websites, applications, and

[1] A full description of USCIS FDNS screening and vetting activities is contained in DHS/USCIS/PIA-013-01 Fraud Detection and National Security Directorate available at www.dhs.gov/privacy.
[2] Use of fictitious accounts means using identities or credentials on social media that do not identify a DHS/USCIS affiliation, or otherwise concealing a government affiliation, to conduct research. Use of fictitious accounts also serves an essential operational security (OPSEC) measure by protecting USCIS employees and DHS IT systems from individuals or groups who may wish to do harm to one or both. Use of fictitious accounts or identities includes logging in to social media, but does not include engaging or interacting with individuals on or through social media.
[3] USCIS places a high priority on detecting, investigating, and preventing immigration fraud. Immigration fraud poses a substantial threat to national security and public safety because it creates a vulnerability that may enable terrorists, criminal aliens, and foreign nationals without lawful immigration status to gain entry to and remain in the United States.
[4] For purposes of this document, the term "immigration request" includes all benefit requests (as that term is defined in 8 CFR 1.2) as well as other immigration-related requests handled by USCIS that are not considered benefits (e.g., deferred action). The term "requester" means someone who has filed an immigration request.
[5] *See* DHS/USCIS/PIA-013-01 FDNS Directorate, *available at* www.dhs.gov/privacy, for a comprehensive list of

web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact."[6]

As described in the DHS/USCIS/PIA-013-01 FDNS Directorate PIA and aligned with FDNS's existing authorities, FDNS Immigration Officers (IOs) may view and gather information from social media sources to fulfill the USCIS mission of enhancing national security and the integrity of the legal immigration systems. FDNS may use fictitious accounts or identities for social media research when necessary in support of the following FDNS mission areas:

Identifying threats posed by those requesting immigration benefits: FDNS IOs conduct security and background checks of immigration requests, in order to identify individuals associated with those requests who may pose a threat to the national security or public safety, or may be otherwise ineligible for immigration requests they are seeking for themselves or others. These checks include searches in government-owned systems of records, but may also include review of open source and publicly available social media information. This includes conducting checks on certain form types or groups of immigration requests, as a matter of policy, or based on an articulated justification.[7]

Detecting, pursuing, and deterring immigration request fraud: During the adjudication of immigration requests, USCIS may discover indicators of potential fraud, criminal, public safety, or national security concerns. Cases in which these concerns are identified are referred to local FDNS IOs for further checks or an administrative investigation. Further checks may also include additional background, identity, or security checks, to include social media checks, as determined by FDNS IOs with the approval of an FDNS supervisor, or at the request of USCIS management or USCIS immigration officers adjudicating immigration requests.

Identifying and removing systemic vulnerabilities in the process of the legal immigration system: In order to identify opportunities for the best use of scarce resources, FDNS IOs conduct, or assist others in conducting, studies and analyses of benefit fraud and other systemic threats to the legal immigration systems. This work sometimes involves randomly selecting previously-adjudicated cases for review after adjudication, and reviewing or re-conducting parts of the security check process when there is an articulable basis for suspecting fraud or systematic threat to the U.S. immigration system.[8] The use of open source and publicly available social media in

sources used by FDNS.

[6] DHS Instruction 110-01-001 Privacy Policy for the Operational Use of Social Media, *available at* https://www.dhs.gov/privacy.

[7] Articulated is defined as having a possible threat to national security, public safety, or a fraud concern. Fraud will be deemed articulated if there is a reasonable suspicion of fraud, or willful misrepresentation of a material fact in connection with an immigration-related benefit. When national security, public safety, or a fraud concern has been articulated, creation of a Case in FDNS-DS may be warranted.

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

these cases would be used to identify any such information that might have had an impact on an adjudication had it been known at the time the immigration request was adjudicated. These studies also help to identify fraud trends, to confirm effectiveness of security checks, and to validate efficacy of the adjudication process. In certain circumstances, information uncovered in a study might lead to further action in individual cases; for example, new evidence of fraud might lead to an investigation, and/or, where appropriate, revocation or rescission of the benefit.

Social media checks are designed to identify publicly available information in social media postings that may impact eligibility. This could include information indicating potential fraud (such as identity fraud or document fraud), or information regarding criminal activity or national security concerns that would impact eligibility and admissibility. USCIS requires the ability to consider that information as it may contradict or substantiate information provided to USCIS in connection with the immigration request.

In compliance with DHS Directive 110-01, Privacy Policy for Operational Use of Social Media and Instruction 110-01-001,[9] USCIS requires FDNS IOs to complete initial USCIS Privacy Requirements for the Operational Use of Social Media training and program-specific training on the authorized use of social media. These trainings, which specifically address the use of fictitious accounts, must be completed prior to accessing social media and renewed on an annual basis. Furthermore, users must sign a "Rules of Behavior (ROB)" form prior to the engagement of social media for FDNS mission-related activities, and renew the ROB annually to continue the use of social media in support of its mission.

With this update, USCIS is documenting FDNS's planned use of fictitious accounts or identities during the course of its access and review of publicly available information on social media. As stated above, FDNS IOs may use fictitious accounts or identities for purposes of (1) identifying threats posed by those requesting immigration benefits; (2) detecting, pursuing, and deterring immigration request fraud; and (3) identifying and removing systemic vulnerabilities in the process of the legal immigration system, as described above. Social media reviews FDNS conducts include a combination of overt research and the use of fictitious accounts or identities.[10] FDNS may only use fictitious accounts or identities to review the requester's publicly available social media accounts with supervisory approval, and in accordance with DHS Delegation 15002, which is included as an Appendix to this PIA. Under no circumstance will USCIS violate any individual's social media privacy settings in the course of reviewing the publicly available social

[9] *See* DHS Directive 110-01, Privacy Policy for Operational Use of Social Media and Instruction 110-01-001, *available at* https://www.dhs.gov/privacy. This Directive sets privacy policy and requirements for DHS and its components for the access, collection, use, maintenance, retention, disclosure, deletion, and destruction of PII in relation to operational use of social media.

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

media information.

FDNS relies on the IO's supervisor to be responsible for authorizing and overseeing creation of any fictitious account or identity. The supervisor maintains the ability to review use of the fictitious account or identity. FDNS IO supervisors are also responsible for maintaining a log of the fictitious accounts or identities when an FDNS IO is using the account. The FDNS IO is responsible for using and managing the accounts in accordance with the Fraud Detection and National Security Investigations ROB for the Operational Use of Social Media. Use of fictitious accounts or identities are subject to routine or for cause audits by FDNS or USCIS leadership, the USCIS Office of Privacy, the Office of Security and Integrity, or privacy compliance reviews by the DHS Privacy Office.

The creation of fictitious accounts or identities to access social media sites to view content that is publicly available to all users of the social media platform is a change from the DHS/USCIS/PIA-013-01 FDNS Directorate PIA, though all other aspects of social media collection and use remain the same. FDNS IOs must use government-issued equipment to access social media. FDNS IOs will not communicate with users of social media sites and may only passively review information that is publicly available to all users of the social media platform. Further, any information found on a social media site that is used in an investigation or adjudication, is required to be recorded and saved in appropriate systems of records, including the applicant's Alien File and FDNS-DS.[11]

In the event social media content that is relevant to the adjudication of the immigration request is found, 8 CFR 103.2(b)(16)(i) provides that an applicant or petitioner should be given an opportunity to review and rebut (e.g., via an interview or in response to a request for evidence or notice of intent to deny) derogatory information of which the applicant or petitioner is unaware, before a final decision based on such derogatory information is made, provided an exemption does not apply (e.g., the information is classified). As a matter of policy, DHS does not use social media information as the sole basis for the denial of any immigration request with the exception of certain discretionary overseas adjudications.

Reason for the PIA Update

FDNS is updating this PIA to provide notice that officers may use fictitious accounts or identities on social media platforms to protect national security, public safety, or to combat immigration fraud, with supervisory approval, and in accordance with DHS Delegation 15002, to

[11] The Alien File is the official record system that contains information regarding the transactions of an individual as he or she passes through the U.S. immigration and inspection process. The A-File system of records (SORN) was updated in 2017 to allow for the collection of social media handles, aliases, associated identifiable information, and search results.

view publicly available information on that site. The creation and use of fictitious accounts or identities enhances operational security (OPSEC).[12] The creation and use of the fictitious accounts or identities does not change the amount of or type of information an IO was previously able to view and collect.

When using fictitious accounts or identities to view publicly available information on social media sites, FDNS IOs will continue to use government-issued equipment. FDNS IOs will respect privacy settings and access only content that is publicly available to all users of the social media platform; view information passively and not communicate with social media users; collect the minimum amount of personally identifiable information (PII) necessary in the proper performance of authorized duties; safeguard PII as required by the Privacy Act and DHS privacy policy;[13] document operational use of social media; and complete annual privacy training, and rules of behavior requirements.

The DHS Privacy Office's statutory mission is to "ensure that the use of technology sustains, and does not erode, privacy."[14] Due to the privacy risks associated created by using fictitious accounts or identities on social media platforms and the scoping of the program, the DHS Privacy Office has included additional recommendations throughout the "Privacy Impact Analysis" section of this PIA to better mitigate the privacy risks associated with FDNS's use of these fictitious accounts or identities as it deploys its social media program. In addition, the DHS Privacy Office will initiate a Privacy Compliance Review (PCR) of FDNS's use of fictitious accounts or identities on social media platforms within 12 months after this PIA is published.[15] The PCR will evaluate how USCIS is protecting privacy as described in this PIA and will also determine if FDNS is following the DHS Privacy Office recommendations provided in the "Privacy Impact Analysis" section of this PIA.

[12] DHS Management Directive 11060.1, Operations Security Program, September 25, 2006, provides that "OPSEC is a systematic and proven process by which U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities". OPSEC encompasses steps taken to protect DHS systems and personnel.
[13] *See* DHS Privacy Policy Guidance Memorandum 2017-01: *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of PII,* available at www.dhs.gov/privacy.
[14] *See* 6 U.S.C. § 142.
[15] *See* DHS Instruction 110-01-001 and DHS Instruction 047-01-004, *available at* https://www.dhs.gov/privacy.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

The legal authority to collect this information comes from the Immigration and Nationality Act, 8 U.S.C. Section 1101 *et seq*., specifically, the Secretary of Homeland Security in Homeland Security Delegation No. 0150.1 delegated the following authorities to USCIS:

> "(H) Authority under section 103(a)(1) of the Immigration and Nationality Act of 1952, as amended (INA), 8 U.S.C. §1103(a)(1), to administer the immigration laws (as defined in section 101(a)(17) of the INA).
>
> (I) Authority to investigate alleged civil and criminal violations of the immigration laws, including but not limited to alleged fraud with respect to applications or determinations within the Bureau of Citizenship and Immigration Services (BCIS) [USCIS] Customs and Border Protection (CBP) or the CIS and make recommendations for prosecutions, or other appropriate action when deemed advisable."[16]

In June 2003, USCIS was delegated the authority to investigate alleged civil and criminal violations of the immigration laws, not limited to alleged fraud with respect to immigration requests or determinations.[17] In January 2017, former Secretary Johnson reaffirmed the authority of USCIS to protect the national security and public safety, to conduct certain law enforcement activities, including accessing social media websites using a fictitious account or identity to view publicly available information.[18] Per that delegation, such activities shall only be conducted by properly trained and authorized officers, in a manner consistent with the reservations set forth in Department of Homeland Security Delegation Number 0150.1 and consistent with the Department's obligations to protect privacy and civil rights and civil liberties. On March 28, 2017, the USCIS Director re-delegated this authority to the Associate Director for FDNS to be exercised by officers and employees within or detailed to FDNS. FDNS investigations may relate to articulable public safety, national security, or fraud concerns with an immigration request, which generally differ from the background checks performed by USCIS adjudicative personnel. Consistent with FDNS's delegated authorities, this use of fictitious accounts or identities includes

[16] Initially named "Bureau of Citizenship and Immigration," or BCIS, the agency was quickly renamed U.S. Citizenship and Immigration Services (USCIS).
[17] *See* Secretary of Homeland Security Delegation No. 0150.1, Section II (H) and (I), for more information.
[18] *See* Secretary of Homeland Security Delegation No. 15002, Delegation to the Director of U.S. Citizenship and Immigration Services to Conduct Certain Law Enforcement Activities. As described in footnote 2, fraud detection, investigation and prevention are integral parts of the DHS (USCIS) mission to protect the national security and public safety of the Homeland.

logging in to and searching social media, but does not include engaging or interacting with individuals on or through social media or accessing any posted information that would otherwise not be available to all users of the social media platform.

The Privacy Act, 5 U.S.C. § 552a(e)(7) provides that an agency maintain no record describing how any individual, (defined in the Act as a U.S. citizen or Lawful Permanent Resident)[19] exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity. USCIS may collect information pertaining to First Amendment activity based on its authority to administer immigration laws as long as such activity is relevant to the specific immigration request adjudication under consideration.[20] On May 17, 2019, Acting Secretary McAleenan reaffirmed that individuals' First Amendment rights are protected regardless of the medium of their communications.[21] Further, USCIS may collect and maintain information pertaining to First Amendment activity as long as such collection is conducted within its delegated authority by the Secretary to conduct certain law enforcement activities, particularly through its re-delegation to USCIS FDNS.[22]

---

[19] 5 U.S.C. § 552a(a)(2).

[20] Privacy Act Implementation, Guidelines and Responsibilities, 40 Fed. Reg. 28,948, 28,965 (July 9, 1975) (hereinafter OMB Guidelines). The Guidelines specifically cite to the Immigration and Nationality Act (INA) as an example of express statutory authorization: "[S]ince the Immigration and Nationality Act makes the possibility of religious or political persecution relevant to a stay of deportation, the information on these subjects may be admitted in evidence, and therefore would not be prohibited by [subsection (e)(7)." OMB Guidelines, at 28,965. Many other INA provisions potentially involve consideration of First Amendment activity. E.g., 8 U.S.C. 1101(a)(43) (definition of refugee, for purpose of refugee and asylum eligibility determinations, includes persecution based on membership in social group, religion, or political opinion); 8 U.S.C. 1182(a)(3)(B) (inadmissibility of any alien who, inter alia, "endorses or espouses terrorist activity or persuades others to endorse or espouse terrorist activity or support a terrorist organization"); 8 U.S.C. 1182(a)(3)(D) (ground of inadmissibility for membership or affiliation with the Communist or other totalitarian party); 8 U.S.C. 1182(a)(3)(F) (ground of inadmissibility for association with terrorist organizations); 8 U.S.C. 1227(a)(4)(B) (deportability of aliens admitted to the United States if described in terrorism-related grounds of inadmissibility); 8 U.S.C. 1424 (prohibition upon the naturalization of persons opposed to government or law, or who favor totalitarian forms of government). DHS/USCIS may also collect this information pursuant to its statutory authority in determining whether the applicant comes under section 313 of the INA's (8 U.S.C. 1424) prohibition upon the naturalization of persons opposed to government or law, or who favor totalitarian forms of government. Thus, collecting and maintaining this information is lawful both because of express statutory authorization as described above, and because the applicant consented to providing it by signing and filing the application.

[21] *See* Secretary of Homeland Security Memorandum, Information Regarding First Amendment Protected Activities, *available at* https://www.dhs.gov/sites/default/files/publications/info_regarding_first_amendment_protected_activities_as1_signed_05.17.2019.pdf.

[22] DHS may still maintain records consistent with 5 U.S.C. § 552a(e)(7) even if there is no ongoing or current law enforcement investigation.

The following SORNs apply to most collection, maintenance, and sharing of information by FDNS, including information obtained through social media sites:

- DHS/USCIS-006 Fraud Detection and National Security Records (FDNS);[23] and
- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records.[24]

The primary case management system for FDNS records is FDNS-DS. FDNS-DS has an approved National Archives and Records Administration (NARA) retention schedule (N1-566-08-18). In addition to FDNS-DS, FDNS uses an unclassified, restricted SharePoint-as-a-Service repository to manage internal policy and operational documents, content, and other information relating to cases.[25]

Characterization of the Information

There is no change to the characterization of the information, as this update does not change the underlying information being viewed or collected from social media sites. As stated in the DHS/USCIS/PIA-013-01 FDNS Directorate PIA, FDNS only collects publicly-available information from social media, and other internet sources related to immigration requests filed with USCIS. FDNS may use fictitious accounts or identities to conduct checks when necessary in support of the FDNS mission areas identified herein. FDNS's use of fictitious accounts or identities will not change the type or amount of information collected on social media sites when logged in.

FDNS only collects social media information that is reasonably related to matters under USCIS consideration. FDNS IOs collect information on individuals during the review of possible national security concerns, public safety threats, or indications of fraud. Information may also be used to corroborate the veracity of information provided by the applicant or petitioner. FDNS IOs only view information passively, do not communicate with social media users, and collect the minimum amount of information necessary to perform authorized duties. If and when FDNS IOs collect social media information as part of the uses described above, FDNS IOs only collect information that is relevant to a pending or previously adjudicated immigration request, and that is tied to the legal standards for that request. FDNS retains information relevant to an administrative investigation in FDNS-DS, and only when information is found to be relevant to the adjudication of an immigration request is it shared with adjudications personnel and retained in the appropriate systems of record.

[23] *See* DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).
[24] *See* DHS/USCIS/ICE/CBP-001-Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).
[25] *See* DHS/ALL/PIA-059 Employee Collaboration Tools, *available at* www.dhs.gov/privacy.

Privacy Risk: There is a risk with social media collection that FDNS IOs will collect more information than necessary or that irrelevant information will be retained.

Mitigation: Individuals maintain control of their own social media privacy settings and can generally choose what information is made public versus what can only be seen by "friends" or "followers." FDNS will respect users' privacy settings for information posted on social media sites, and will not "friend" or "follow" the individual to gather more information, consistent with DHS Directive 110-01. FDNS only views and gathers publicly available information from social media sources to fulfill the USCIS mission of enhancing both national security and the integrity of the legal immigration system by: (1) identifying threats posed by those submitting immigration requests; (2) detecting, pursuing, and deterring immigration benefit fraud; and (3) identifying and removing systemic vulnerabilities in the process of the legal immigration system. FDNS reviews information from multiple sources in order to have the best evidence available to make a determination on a case. Supervisory review of every case and routine or for-cause auditing help to ensure that only the minimal amount of information relevant to an administrative investigation or adjudication is accessed and retained in the appropriate systems of record.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends that the USCIS Office of Privacy regularly interact with FDNS employees to ensure privacy protections are maintained to ensure that only the minimum information required is collected and maintained.

Uses of the Information

FDNS collects information on individuals during the review of possible national security concerns, public safety threats, or indications of fraud related to applications for immigration benefits. Information may also be used to corroborate the veracity of information provided by the applicant or petitioner. FDNS IOs document the official social media findings including, what information was gathered, and how the information was used, within FDNS-DS. FDNS IOs may use access-controlled pages on the USCIS Enterprise Collaboration Network or shared drives to create and edit working documents before storing the official and approved version in FDNS-DS.[26] FDNS uses publicly available social media information to confirm whether the public information is consistent with information provided in the immigration request, to build lines of inquiry when requesting in-person interviews, or to assist USCIS adjudications personnel in formulating a Request for Evidence (RFE) or a Notice of Intent to Deny (NOID) to the applicant or petitioner. When relevant social media information needs to be shared with adjudications personnel, this is memorialized through official documentation such as a Statement of Findings (SOF).

[26] The USCIS ECN is built using SharePoint, which is a document management and collaboration tool developed by Microsoft. SharePoint is a commercial off-the-shelf (COTS) that provides a cloud-based platform to build custom applications and features a suite of collaboration, document management, and communication tools.

USCIS generally allows the applicant or petitioner the opportunity to explain and resolve any inconsistencies among information sources before USCIS issues an adjudicative decision. If USCIS determines information obtained from social media of which the applicant or petitioner is unaware is relevant to the adjudication, resulting in a potential adverse decision, the applicant or petitioner will have the opportunity to explain and resolve any inconsistencies among information sources prior to issuance of an adjudicative decision.[27] With limited exceptions, the applicant, petitioner or requestor will have an opportunity to file a motion or an appeal if the immigration request is denied.[28]

As a matter of policy, DHS does not use social media information as the sole basis for the denial with the exception of certain discretionary overseas adjudications. Further, not all information obtained from social media is considered derogatory. There are cases in which FDNS IOs uncover information of interest that confirms the veracity of information provided by the applicant or petitioner in the case.

FDNS does not currently apply algorithms or advanced analytics to collect or analyze social media. USCIS will update this PIA prior to any bulk ingestion, use of algorithms, or application of advanced analytics to social media.

There are no new privacy risks associated with this use as it remains unchanged from the DHS/USCIS/PIA-013-01 FDNS Directorate PIA.

DHS Privacy Office Recommendation: As with all tools and techniques that can be privacy sensitive, the DHS Privacy Office recommends that fictitious accounts or identities only be used when there is an articulated need for a fictitious account. Fictitious accounts or identities should not be the default option.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends that FDNS personnel document each case that is researched using social media, the FDNS personnel's account that was used to conduct the search, what information was gathered, and how it was used in the same manner that FDNS would document information collected from any source in the normal course of business.

Notice

This PIA, as well as other USCIS PIAs, provides notice to the individual that FDNS may access an individual's public social media content during the course of the immigration adjudication process.

Privacy Risk: There is a risk that FDNS does not provide sufficient notice to individuals

[27] 8 CFR 103.2(b)(16).
[28] 8 CFR. 103.3(a)(1)(ii) and 103.5. Also, in the Refugee context, an applicant may file a Request for Review as described in the Refugee Request for Review Tip Sheet available at http://www.uscis.gov.

who are not seeking immigration benefits or who are not subject to an administrative investigation by FDNS.

Mitigation: This risk is partially mitigated. FDNS's access and use of publicly available information is relevant to the adjudication of immigration benefits (such as when information provides evidence of an individual's persecution claim; when an individual may be inadmissible or otherwise ineligible for an immigration benefit due to an affiliation with a known terrorist organization or criminal gang; or when an individual is involved in large-scale immigration fraud). As part of the administrative investigation, FDNS may view the subject's profiles and collect content that is publicly available to all users of the social media sites. In the course of this collection, FDNS may also obtain publicly-available information from an associate of the subject under investigation, such as comments left on an image that is relevant to an open investigation. In such cases, FDNS might collect the comment itself and the listed screen name of the individual leaving the comment, in the process of collecting the post of the subject under investigation, relevant to the specific immigration benefit adjudication under consideration. FDNS would only actively seek information relevant to an ongoing investigation. While USCIS may collect information related to these individuals, USCIS only collects social media information that is reasonably related to matters under USCIS consideration.

Through the social media site's respective privacy policy, individuals who post content on social media are advised that any information shared in a public forum is considered publicly available information. This is an inherent risk to the general use of social media.

USCIS cannot provide direct notice to associates not seeking immigration benefits or an individual subject to an administrative investigation by FDNS because providing notice may hinder FDNS's ability to effectively complete the administrative investigation. The publication of this PIA, other FDNS PIAs, and the relevant SORNs provide general transparency and notice into FDNS's use of social media.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends that USCIS collect metrics related to the data quality, integrity, and uses of this information under this program. More meaningful data about the program will provide USCIS the ability to share additional information about how the program works with the public.

Data Retention by the project

There is no change to retention of information. FDNS continues to maintain information pursuant to the records retention schedule for the underlying system of records (typically FDNS-DS or the Alien File) as described in the DHS/USCIS/PIA-013-01 FDNS Directorate PIA.

Information Sharing

There is no change to internal or external sharing of this information, as this update does

not change the underlying information being viewed and how it is used or shared. Any disclosures are made pursuant to routine uses allowable in the FDNS SORN and are compatible with the original collection because the INA requires USCIS to investigate alleged civil and criminal violations of immigration laws, including alleged fraud with respect to immigration requests or determinations within USCIS.

DHS Privacy Office Recommendation: Due to the inherent data accuracy concerns associated with collecting information from social media, the DHS Privacy Office recommends that USCIS make reasonable effort to ensure the accuracy of the information. In doing so, FDNS must ensure that any PII shared external to the Department is for a purpose compatible with the purpose for which the information was collected.[29]

Redress

The individual right to access, redress, and correction has not changed with this update. Individuals maintain the right to file a Freedom of Information Act (FOIA) request to gain access to USCIS records. U.S. citizens, lawful permanent residents, and covered persons with covered records under the Judicial Redress Act[30] may file a Privacy Act request to gain access or amend their erroneous data. Any individual seeking to access information maintained by FDNS should direct his or her request to USCIS National Records Center (NRC), P.O. Box 648010, Lee's Summit, MO 64064-8010.

When USCIS determines information obtained from social media is relevant to the adjudication of an immigration request, the FDNS IO can provide information found in open sources for USCIS adjudications personnel to formulate an RFE, a NOID to the applicant or petitioner, or during an interview with the petitioner and/or beneficiary. The applicant and/or petitioner will have the opportunity to explain and resolve any inconsistencies among information sources of which he or she is unaware prior to issuance of an adjudicative decision if the decision is adverse and if it is based on that derogatory information. With limited exceptions, the applicant and/or petitioner will have an opportunity to file a motion or an appeal if the application or petition is denied.

Privacy Risk: While the individual right to access, redress, and correction has not changed with FDNS's use of fictitious social media accounts, there is a risk that non-immigrants will not be able to access or amend their records.

Mitigation: This risk is partially mitigated. Any individual, regardless of immigration status, may file a request to access his or her information under FOIA. To the extent information is not exempt under FOIA, DHS is required to produce the information. In addition, prior to DHS

[29] *See* Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information," *available at* www.dhs.gov/privacy.
[30] Judicial Redress Act of 2015, Pub. L. 114-126, codified at 5 U.S.C. 552a note.

making a determination to deny an immigration request, when information is to be used as part of the basis for a denial, DHS will share the information with the individual and offer him or her the opportunity to address and correct the information.

Auditing and Accountability

All authorized FDNS IOs receive the USCIS Privacy Requirements for the Operational Use of Social Media training and sign Rules of Behavior, which specifically address the use of fictitious accounts, before initial use is granted and annually thereafter. FDNS IOs also receive annual privacy awareness and program-specific training that reinforces the privacy principles. Authorized FDNS IOs may use fictitious accounts or identities when there are possible and articulable national security, public safety, or immigration fraud concerns. FDNS IOs may use fictitious accounts or identities to protect the national security and public safety, when there are fraud concerns, or as a matter of policy based on an articulated justification with the approval of their supervisor, and in accordance with DHS Delegation 15002 USCIS FDNS's required social media training specifically addresses the use of fictitious accounts and how to identify First Amendment activity and determine if social media posts discuss protected activities or relevant to USCIS's uses described above. All FDNS IOs who access social media sites, regardless of whether they conduct overt research or use fictitious accounts or identities, are required to complete hands-on training on the proper use of any tools or tradecraft used to access social media sites, and the mandatory annual refresher training.

At this time, USCIS does not permit all FDNS IOs to access social media sites. Only a limited number of IOs are presently permitted to access social media sites. Use of fictitious accounts or identities to access social media sites is further limited to those FDNS IOs who have completed the appropriate training and have supervisory approval. The names of authorized users and their signed agreement to follow the FDNS Rules of Behavior for the Operational Use of Social Media (ROB) will be maintained by the user's manager or supervisor. The IO's supervisor will be responsible for overseeing creation of any fictitious account. The supervisor will maintain an accounting of all fictitious account handles or identities used and will maintain the ability to review use of the fictitious account. Cases involving use of fictitious accounts or identities, to include information accessed using the accounts, will be documented in FDNS-DS.

An authorized user loses authorization upon changing to a position or duties for which the operational use of social media is not authorized. Managers and supervisors will ensure that their respective list of authorized users is up to date. An employee who transfers to a new position or office must be reauthorized by the gaining office if continued operational use of social media is warranted. The USCIS Office of Privacy, directorates, and program offices shall follow current agency practices to document training and compliance agreements.

The USCIS Office of Privacy and other oversight offices will conduct reviews, as needed,

of processes and procedures related to use of fictitious accounts or identities on social media. Finally, the use of fictitious accounts or identities to access publicly available social media content will be subject to routine audit 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.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends that USCIS FDNS implement a review cycle to regularly confirm the efficacy placed on collecting social media information using fictitious accounts or identities for the purposes of reviewing immigration requests. This will ensure that information is being used to support mission requirements.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends that USCIS require requests for social media accounts be reviewed and renewed on an annual basis.

Responsible Officials

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A

Department of Homeland Security
DHS Delegation Number: 15002
Revision Number:
00 Issue Date:
1/19/2017

DELEGATION TO THE DIRECTOR OF U.S. CITIZENSHIP AND IMMIGRATION SERVICES TO CONDUCT CERTAIN LAW ENFORCEMENT ACTIVITIES

I. Purpose

This delegation reaffirms the authority of the Director of U.S. Citizenship and Immigration Services (USCIS) to conduct law enforcement activities including but not limited to accessing internet and publicly available social media content using a fictitious account or identity.

II. Delegation

Subject to my oversight, direction, and guidance, under Department of Homeland Security Delegation Number 0150.1 I have delegated to the Director of USCIS the authority:

> In matters under the jurisdiction of USCIS, to protect the national security and public safety, to conduct law enforcement activities, including but not limited to accessing internet and publicly available social media content using a fictitious account or identity, provided that such activities shall only be conducted by properly trained and authorized officers, and in a manner consistent with the Reservations set forth in Department of Homeland Security Delegation Number 0150.1 and consistent with the Department's obligations to protect privacy and civil rights and civil liberties.

III. Re-delegation

Unless otherwise proscribed by statute, Executive Order, or the terms of this delegation, the powers, authorities, responsibilities, and functions delegated herein may be redelegated in writing by the Director, and may be successively redelegated to other officers or employees of USCIS qualified to exercise the authority.

IV. Authorities

A. Homeland Security Act of 2002, Pub. L. No. 107-296, § 102, 116 Stat. 2135 (2002), as amended (6 U.S.C. § 112).

B. Immigration and Nationality Act of 1952, Pub. L. No. 82-414, § 103(a), 66 Stat. 163, as amended (8 U.S.C. § 1103(a)).

C. 8 C.F.R. § 2.1 (Authority of the Secretary of Homeland Security).

V. Office of Primary Interest

The Office of the Director, USCIS has the primary interest in this delegation.

Jeh Charles Johnson
Secretary of Homeland Security

1/15/17
Date