Privacy Impact Assessment
for the

Continuous Immigration Vetting

DHS/USCIS/PIA-076
February 14, 2019

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

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

In 2017, through an effort known as Continuous Immigration Vetting (CIV), U.S. Citizenship and Immigration Services (USCIS) began vetting information from certain immigration benefit applications throughout the entire application adjudication period as new information is received, rather than only performing point-in-time checks, to further enhance the agency's ability to identify national security concerns. CIV is an event-based[1] vetting tool that automates and streamlines the process of notifying USCIS of potential derogatory information in Government databases that may relate to individuals in USCIS systems, as new information is discovered. USCIS is now incrementally expanding CIV to encompass screening and vetting immigrant and nonimmigrant applications and petitions throughout the duration of the benefit or status, until the individual becomes a naturalized U.S. Citizen. USCIS is publishing this Privacy Impact Assessment (PIA) to provide greater transparency into the CIV initiative and to assess the impact of automating event-based vetting for individuals from the time of an initial benefit filing up until naturalization.

Introduction

USCIS oversees many aspects of lawful immigration to the United States and is responsible for processing petitions, applications, and other requests for immigration benefits. USCIS is responsible for providing the right immigration benefit, to the right person, in the right amount of time. As part of the 2014-2018 Department of Homeland Security (DHS) Strategic Plan, USCIS must enforce immigration laws by:

> *Ensuring that only eligible applicants receive immigration benefits through expanded use of biometrics, a strengthening of screening processes, improvements to fraud detection, increases in legal staffing to ensure due process, and enhancements of interagency information sharing.*[2]

Security and integrity are central to USCIS's mission, and USCIS systematically conducts screening and vetting on every immigrant and nonimmigrant benefit application to identify information that may affect an individual's eligibility for a benefit or admissibility into the United States, and to inform proper adjudicative decisions. During the course of the adjudication process, USCIS completes the following:

---

[1] CIV is "event-based," because it is triggered by an event, such as when new biographic and/or biometric information about an individual is added to USCIS systems (e.g. a new application is filed, fingerprints are taken, or an address is updated).

[2] Department of Homeland Security, *Fiscal Years 2014-2018 Strategic Plan*, September 16, 2015, https://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF.

- **Background checks** to obtain relevant information so that USCIS may render the appropriate adjudicative decision with respect to the application or benefit;
- **Identity checks** to confirm the individual's identity and combat potential fraud; and
- **Security checks** to identify potential threats to public safety or national security.

USCIS uses several USCIS and DHS systems to support the checks identified above. For example, USCIS conducts biographic-based checks against TECS[3] (not an acronym) and biographic and biometric-based checks using systems such as the Customer Profile Management System[4] and the DHS Automated Biometric Identification System (IDENT).[5] Also, the types of checks required vary depending on the type of immigration or non-immigration application or petition and are described in detail in PIAs conducted for the specific USCIS and DHS screening and case management systems, as well as USCIS programmatic PIAs for certain immigration benefits.[6] Ultimately, conducting these checks ensures that benefits are granted only to eligible individuals who do not pose a threat to national security or public safety, and who are not engaged in benefit fraud.

Historically, USCIS staff had to perform manual, point-in-time checks of various systems in order to accomplish the full suite of required checks for a given application or petition. In 2014, USCIS Fraud Detection and National Security Directorate (FDNS) developed a platform called ATLAS to automate and streamline the screening of biographic and biometric information received from immigration benefit applicants.[7] ATLAS has the ability to compare application information against customs, immigration, terrorism, and counterterrorism information held in U.S. Government systems using computer automation, rather than manual system checks, to identify potential derogatory information that matches entries in DHS vetting systems as new information is discovered, and to preemptively notify USCIS personnel with a role in the immigration vetting process. As described in the FDNS-DS PIA, ATLAS screens applicant information against DHS systems that contain derogatory information, applies rules to standardize how potential derogatory information is analyzed, and refers matches to a USCIS immigration application or petition information back to FDNS via a system-generated notification (SGN). ATLAS enhances USCIS's ability to detect derogatory concerns earlier in the vetting process of immigration petitions and applications and supports USCIS in quickly identifying potential cases of national security, public safety, and fraud. While USCIS has the administrative authority, responsibility, and jurisdiction to identify potential cases of national security, public safety, and fraud, USCIS may ultimately refer these cases to U.S. Immigration and Customs Enforcement

[3] DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).
[4] DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS), available at www.dhs.gov/privacy.
[5] DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), available at www.dhs.gov/privacy.
[6] All USCIS PIAs are available at www.dhs.gov/privacy.
[7] *See* DHS/USCIS/PIA-013(a) FDNS-DS, *available at* www.dhs.gov/privacy.

(ICE) for criminal investigation or enforcement action, as part of ICE's criminal investigative authority.

With the efficiencies and successes achieved with the deployment of ATLAS, USCIS recognized the value of using computer automation, rather than continuing to rely on multiple manual, point-in-time checks, to identify potential derogatory matches within U.S. Government databases and vetting systems as new information is discovered. Executive Order (EO) 13780, *Protecting the Nation from Foreign Terrorist Entry into the United States*, dated March 16, 2017, reaffirmed the need for this automated capability. The EO directed the implementation of a program to identify individuals who seek to enter the United States on a fraudulent basis, who support terrorism, violent extremism, acts of violence toward any group or class of people within the United States, or who present a risk of causing harm subsequent to their entry. As further clarified in Section 5(a):

> *"This program shall include the development of a uniform baseline for screening and vetting standards and procedures, such as in-person interviews; a database of identity documents proffered by applicants to ensure that duplicate documents are not used by multiple applicants; amended application forms that include questions aimed at identifying fraudulent answers and malicious intent; a mechanism to ensure that applicants are who they claim to be; a mechanism to assess whether applicants may commit, aid, or support any kind of violent, criminal, or terrorist acts after entering the United States; and any other appropriate means for ensuring the proper collection of all information necessary for a rigorous evaluation of all grounds of inadmissibility or grounds for the denial of other immigration benefits."*[8]

In furtherance of the EO and consistent with the Immigration and Nationality Act, 8 U.S.C. Section 1101 *et seq*., USCIS is working with U.S. Customs and Border Protection (CBP) and ICE to develop Continuous Immigration Vetting (CIV), a vetting capability that applies uniform screening and vetting standards across identified immigrant and nonimmigrant populations and will vet applicants and beneficiaries from the time of the initial immigration filing, through the duration of the benefit or status, until the individual becomes a naturalized U.S. citizen. CIV leverages the successes realized with ATLAS and connects ATLAS to CBP's Automated Targeting System (ATS)[9] to conduct checks against CBP holdings, to further automate and streamline the vetting process.

---

[8] Federal Register, *Executive Order 13780, Protecting the Nation from Foreign Terrorist Entry into the United States*, March 6, 2017, https://www.federalregister.gov/documents/2017/03/09/2017-04837/protecting-the-nation-from-foreign-terrorist-entry-into-the-united-states, Section 5.

[9] *See* DHS/CBP/PIA-006(b) Automated Targeting System (ATS), *available at* www.dhs.gov/privacy.

USCIS currently conducts background, identity, and security checks on individuals connected to immigration applications and petitions, including both manual and automated point-in-time checks through ATLAS. ATLAS's automated checks are triggered by an event, such as an individual filing an application with USCIS or the receipt of new biographic, biometric, or potentially derogatory information. CIV enhances current processes by leveraging ATLAS's ability to automate the detection of new, potentially derogatory information, checking available datasets in ATS, and applying a consistent vetting approach to identified immigrant and nonimmigrant populations. ATLAS provides immediate notification to USCIS as new information is discovered within Government databases and potentially derogatory matches are made – rather than relying on manual, point-in-time checks to discover new information that may affect the eligibility or status of an applicant or beneficiary.

This intra-agency effort allows USCIS:

- To conduct event-based, automated checks of information in CBP holdings that matches to individuals connected to a USCIS immigration application up until an individual is naturalized.
- To apply a uniform process to identify derogatory information that indicates potential threats to national security (and eventually public safety and fraud), as it is received.
- To react more quickly to derogatory information and to refer information to ICE for further investigation in cases that may result in enforcement action.

Systems

To support a uniform vetting and notification process, USCIS and CBP established a connection between USCIS ATLAS and CBP's ATS. This connection serves as the primary conduit to send USCIS application data to CBP for checks against its holdings and for CBP to send results and notifications when new or changed information is discovered to USCIS for validation and review by USCIS, and to ICE, when necessary, for criminal investigation or enforcement action.

ATS is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments. For the purpose of this program, ATS is used to assist USCIS in vetting of immigration benefit applicants for national security.

ATLAS is a USCIS platform that facilitates screening biographic and biometric information received from immigration benefit filings and uses rule-based computer automation to identify potential derogatory matches to records in DHS systems that indicate potential fraud, public safety, or national security concerns. This information is further discussed in the Fraud

Detection and National Security – Data System (FDNS-DS)/ATLAS PIA.[10] CBP also maintains an Addendum to the ATS PIA to discuss ATS's use as a conduit to assist USCIS with immigration vetting.[11]

ATLAS makes use of information obtained through existing interfaces with USCIS and DHS immigration case management and screening systems to transmit biographic data from or associated with immigration benefit filings to CBP ATS for vetting. The IT systems that facilitate CIV are included in Appendix A to this PIA. These system interfaces allow ATLAS to receive adjudication status updates and provide notification to ATS when an individual has naturalized and vetting should stop.

Currently, when criminal investigation or enforcement action is deemed necessary, USCIS manually sends referrals to ICE. Upon sending to ICE for investigation, ICE will handle the records in accordance with its investigatory standard operating procedures and the various laws on counterterrorism and national security that permit the sharing of the information. This includes ICE potentially sharing information with federal, state, tribal, local and foreign law enforcement agencies, as well as relevant law enforcement fusion centers, or external partners that have a demonstrated law enforcement, intelligence, or national security need to know. USCIS is working with ICE to develop an automated process to electronically send referrals to ICE via ATLAS when derogatory information is identified and referred for possible enforcement action. USCIS will update this PIA to document this automated process.

Certain classes of individuals require increased protection to comply with legal, regulatory, or policy requirements. In all cases, USCIS and ICE ensure that sharing of information adheres to the relevant requirements. For example, confidentiality provisions outlined in 8 U.S.C. § 1367 authorize DHS (including USCIS, ICE, and CBP) to access and use Section 1367 information in support of their respective missions. Specifically, 8 U.S.C. § 1367(a)(2) provides that, with certain limited exceptions, DHS is prohibited from disclosing any information relating to an individual who is the beneficiary of an application for T, U, or Violence Against Women Act nonimmigrant status. This includes information about both principals and derivatives, and it covers any information about the individuals, including information provided to USCIS as well as the fact that he or she has applied for or received a benefit. The nondisclosure requirement does not apply to disclosures of protected information within DHS for legitimate agency purposes. Any DHS personnel who manage Section 1367 information, or may come in contact with this information, must receive the appropriate training for identifying and handling protective status cases. Prior to ICE disclosing any information to external entities, ICE will take precautions to ensure the

[10] *See* DHS/USCIS/PIA-013(a) FDNS-DS, *available at* www.dhs.gov/privacy. Information about form intake and initial screening is also included in the various PIAs for the USCIS case management systems and background check systems that make up a part of this process (e.g., CLAIMS 4, ELIS, CPMS).
[11] *See* DHS/CBP/PIA-006(b) Automated Targeting System (ATS) 2.4 Continuous Immigration Vetting Addendum, *available at* www.dhs.gov/privacy.

information is only shared in accordance with the 8 U.S.C § 1367 and DHS policy sharing decisions.

Characterization of the Information

As part of this initiative, immigrant and nonimmigrant applications/petitions are subject to continuous vetting, up to issuance of a naturalization certificate.[12] CIV, in its current implementation, is very limited in scope and is applied to screen identified applications and petitions for potential national security concerns. USCIS is implementing CIV and vetting of identified immigrant and nonimmigrant populations in a phased approach.

In June 2017, USCIS began applying CIV to naturalization applicants through adjudication of the underlying benefit application. In July 2018, USCIS extended CIV to lawful permanent residence applications through adjudication of the underlying application. With the publication of this PIA, USCIS will apply CIV uniformly to identified immigrant and nonimmigrant benefit types from the time of the initial immigration benefit filing, through the duration of the benefit or status, until the individual becomes a naturalized U.S. citizen and is issued a naturalization certificate. For a complete list of immigrant and nonimmigrant benefit types by forms, please see Appendix B to this PIA. USCIS continues to develop CIV in a phased approach and will update this appendix as additional immigrant and nonimmigrant benefit types are added.

The data ATLAS sends to ATS for CIV is derived from the individual's submitted application or petition and may include biographic identifiers such as the applicant name, date of birth, country of residence, etc. In some cases, when additional information is available in the DHS Automated Biometric Identification System (IDENT)[13] (i.e., biographic information, biometric identifiers, or encounter information), ATLAS may enhance USCIS records with that information and include it in the submission to ATS. ATS is already able to retrieve this information through its existing interface with IDENT.

CIV Process

As USCIS is developing this process incrementally, this PIA discusses the process associated with the initial implementation and will be updated to account for future expansions of the program. CIV, in its current implementation, is very limited in scope and is applied to screen application and petition data for potential national security concerns. USCIS is responsible for ensuring that immigration benefits are not granted to individuals that may that pose a threat to national security and that individuals who have been granted benefits remain eligible to maintain that status. CIV allows immigration officers to readily identify certain indicators of a national

[12] USCIS benefits are subject to revocation even post-adjudication if the applicant or petitioner does not meet the immigration benefits eligibility standards.
[13] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.

security concern at any point during the adjudication period of a benefit and up until an individual is naturalized.

A national security concern exists when an individual or organization has been determined to have an articulable link to prior, current, or planned involvement in, or association with, an activity, individual, or organization described in sections 212(a)(3)(A), (B), or (F), or 237(a)(4)(A) or (B) of the Immigration and Nationality Act.[14] This includes terrorist activity; espionage; sabotage; and the illegal transfer of goods, technology, or sensitive information.

The CIV process is initiated when an applicant or petitioner files a benefit application or petition with USCIS. ATLAS sends USCIS application and petition data to ATS to begin vetting. ATS facilitates the automated matching of USCIS application and petition data against CBP holdings and returns vetting results to ATLAS for any appropriate action by USCIS.

CIV is event-based and occurs in two different circumstances. First, when an individual presents him or herself to the agency (i.e., when USCIS receives an individual's application, such as for adjustment of status; when there is an update to an application; or when an applicant's fingerprints are taken at an authorized biometric capture site as part of the form application process), ATLAS sends data to ATS to check CBP holdings for matches to information about individuals who have been identified as posing a threat to national security. CBP retains the USCIS application data in ATS for the duration of vetting under CIV in order to assist USCIS with matching against any new derogatory information identified after the initial application or fingerprinting. Second, when derogatory information is associated with the individual in Government databases that contain information about national security threats, ATS checks to see if there is a match and/or association to the USCIS applicant or petitioner and, in the event of a match, sends the vetting results to ATLAS for further analysis.

When potential derogatory information is matched to a USCIS record, ATLAS receives the ATS vetting results and filters the results through its rules engine to identify possible national security concerns, and then transmits the completed results to the end-user in the form of a SGN, viewable in the FDNS-DS system.[15] SGNs are presented to immigration officers to manually review and verify whether the information relates to the applicant, and whether there is actionable information. Applying ATLAS's predefined rules to the ATS vetting results serves:

- To standardize how information is analyzed.
- To rapidly detect potential derogatory information that may indicate a risk to the nation that would potentially result in an ineligibility determination for an immigration benefit.
- To ensure notifications of derogatory information are only triggered when the results are

[14] 8 U.S.C. § 1182.
[15] See DHS/USCIS/PIA-013(a) FDNS-DS, available at www.dhs.gov/privacy.

relevant and actionable.

- To ensure that the notifications are consistent with legal requirements and DHS and USCIS policy, including all applicable privacy, civil rights and civil liberties protections.

The automated process serves to provide more timely identification and notification of the most serious concerns that could impact national security. Although automation assists with the identification of national security concerns, FDNS officers also manually review each hit to confirm the validity, relevancy, and accuracy of information and to determine if the information is actionable, consistent with DHS authorities. If actionable, USCIS FDNS may perform administrative investigations to produce findings to sufficiently inform adjudications.

When national security concerns are detected after the adjudication of a USCIS benefit (e.g., when new derogatory information is associated with the individual in one or more Government databases, as identified through ATS), USCIS works with ICE to review, assess, and coordinate potential criminal investigation or enforcement action, when appropriate. This review includes an assessment of whether any derogatory information affects the individual's current immigration status and may involve coordination with other law enforcement or intelligence agencies, according to ICE's existing investigatory standard operating procedures and the various laws on counterterrorism and national security that permit the sharing of the information. No operational decisions are based solely on information obtained through CIV. In all cases, USCIS and ICE conduct manual reviews and confirm validity of information retrieved through CIV prior to taking further action based on receipt of potentially derogatory information. FDNS's manual review process is described in the FDNS-DS and Directorate PIAs, and is done in accordance with USCIS standard operating procedures.[16]

Operationally, USCIS uses CIV to automate national security checks. Successful implementation of CIV for national security concerns will inform future efforts to automate CIV for public safety concerns as well as articulated and actionable fraud, consistent with EO 13780.

ATS stops vetting when it receives a message from ATLAS based on a certificate of naturalization issuance. CBP is required to return an acknowledgment of receipt of such notification as well as a "stopped CIV" indicator. With the exception of limited data such as unique system identifiers needed to support auditing capabilities, CBP will not retain this data in ATS after the issuance of the naturalization certificate unless the data is linked to active law enforcement lookout records, enforcement activities, or investigations or cases, in which case that data is maintained by CBP in ATS consistent with the ATS retention schedule as reflected in the ATS SORN (i.e., for the life of the law enforcement matter to support that activity and other enforcement activities that may become related). The limited data otherwise retained in ATS is

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

used solely for auditing purposes, to support USCIS in its ability to conduct in-depth quality reviews.

Governance and Oversight

USCIS has established a governance structure to ensure that ATLAS screening rules are compliant with all legal and privacy requirements. New rules undergo several layers of operational, legal, privacy, and policy review before they are presented to the Deputy Director, USCIS, for final approval. Through this process, FDNS ensures that all screening activity is properly vetted and falls within USCIS's authority. All screening methods deployed are tailored to provide information that is relevant to identifying information that may relate to statutory grounds of inadmissibility found in the INA or that may affect an individual's eligibility for a benefit. USCIS may conduct screening/vetting in situations in which USCIS has the authority to rescind, revoke, or otherwise terminate, to issue a Notice to Appear (NTA), or to refer to another Government agency for criminal/civil actions. Additionally, all information shared is appropriately protected against unlawful use or disclosure in accordance with 8 U.S.C. Section 1367.

Privacy Impact Analysis

USCIS is conducting this PIA to provide additional transparency beyond what was published with the initial launch of this effort in 2017, to account for the risks associated with vetting of application data throughout the duration of the individual's status, until the individual becomes a naturalized U.S. Citizen. This CIV PIA replaces the prior USCIS PIA Appendices and supplements the CBP PIA Addendums previously published for USCIS's and CBP's respective systems (i.e., ATLAS[17] and ATS[18]) and provides a holistic view and assessment of CIV and how it may impact individuals who apply for immigration benefits with USCIS.

USCIS carefully considered the impact this change would have on individuals who are subject to CIV, particularly those who may hold lawful permanent resident status in the United States for an indefinite period of time without filing for naturalization. USCIS designed an event-based vetting model that would pose the least possible impact on individuals' civil rights, civil liberties, and privacy. This allows USCIS to benefit from rapid detection and notification of risks to the security of our nation while ensuring that only those individuals about whom there are significant national security concerns are impacted by the process. In summary, civil rights, civil liberties and privacy mitigations include:

- Narrowly scoped detections of threat indicators in government law enforcement databases. CIV vetting results are filtered through ATLAS's rules engine to ensure notifications are only provided to USCIS in response to events when there is information in Government databases that indicates potential threats to the United States, such as a national security

[17] *See* DHS/USCIS/PIA-013(a) FDNS-DS, *available at* www.dhs.gov/privacy.
[18] *See* DHS/CBP/PIA-006(e) ATS, *available at* www.dhs.gov/privacy.

related law enforcement encounter. Notifications are only produced when existing screening criteria are met, consistent with existing law, USCIS screening policy, and point-in-time checks USCIS has historically performed manually.

- Human review built into the vetting process to confirm matches to USCIS applicant and beneficiary identities, as well as to confirm the validity of potentially derogatory information and its relevance to the individual's eligibility for a benefit or admissibility into the United States.
- Immediate notification of adjudication status updates and a requirement for CBP to purge the USCIS application data from ATS when an individual naturalizes to ensure USCIS does not continue to vet the individual once he or she becomes a U.S. citizen. This also serves to prevent over-collection of USCIS application/petition data in ATS and to prevent any secondary use or potential misuse of information.
- Internal quality controls and review processes to evaluate technical performance, efficacy of the program, and to perform system tuning, when necessary, to ensure vetting results continue to be properly scoped in current operations and throughout any expansion of CIV.
- Close coordination with DHS and component oversight offices to ensure privacy, civil rights and civil liberties, and legal review and concurrence prior this process being applied to any new immigrant and nonimmigrant populations.
- Transparency through this PIA, as well as through notices on USCIS immigration benefit forms and through the public website at USCIS.gov,[19] to notify individuals of the requirements to maintain lawful permanent residence, as well as checks USCIS performs throughout the duration of the individual's status, until naturalization.

This intra-agency effort is being implemented in a phased approach, and as such, DHS will continue to assess the legal, privacy, civil rights and civil liberties, and other policy implications and will update this PIA and relevant system PIAs, when applicable, to account for any expansion.

Individual Rights and Liberties

USCIS is committed to the fair and equal treatment of all individuals in our screening and vetting activities, ensuring the rights of all people while taking lawful actions necessary to secure the homeland. In addition to the framework of protections and privacy mitigations detailed in this PIA, compliance with existing DHS policies will foster the appropriate use of the ATLAS system for CIV purposes. This includes adherence to the existing DHS policy that prohibits the consideration of race or ethnicity in investigation, screening, and law enforcement activities in all

[19] *See* "Maintaining Permanent Residence," accessible from https://www.uscis.gov/green-card/after-green-card-granted/maintaining-permanent-residence.

but the most exceptional instances and limits the consideration of an individual's simple connection to a particular country, by birth or citizenship, as a screening criterion to situations in which such consideration is based on an assessment of intelligence and risk and in which alternatives do not meet security needs. Accordingly, USCIS vetting activities carried out through the ATLAS system, including CIV, may not be used to collect, access, use, or retain information on an individual solely on the basis of actual or perceived race, ethnicity, or nationality. The following is the Department's policy:[20]

> "Racial profiling" is the invidious use of race or ethnicity as a criterion in conducting stops, searches, and other law enforcement, investigation, or screening activities. It is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity. The Department of Homeland Security (DHS) has explicitly adopted the Department of Justice's "Guidance Regarding the Use of Race by Federal Law Enforcement Agencies," issued in June 2003. It is the policy of DHS to prohibit the consideration of race or ethnicity in our daily law enforcement and screening activities in all but the most exceptional instances, as defined in the DOJ Guidance. DHS personnel may use race or ethnicity only when a compelling governmental interest is present, and only in a way narrowly tailored to meet that compelling interest. Of course, race or ethnicity-based information that is specific to particular suspects or incidents, or ongoing criminal activities, schemes or enterprises, may be considered, as stated in the DOJ Guidance.
>
> Except as noted below, it is DHS policy, although not required by the Constitution, that tools, policies, directives, and rules in law enforcement and security settings that consider, as an investigative or screening criterion, an individual's simple connection to a particular country, by birth or citizenship, should be reserved for situations in which such consideration is based on an assessment of intelligence and risk, and in which alternatives do not meet security needs, and such consideration should remain in place only as long as necessary. These self-imposed limits, however, do not apply to antiterrorism, immigration, or customs activities in which nationality is expressly relevant to the administration or enforcement of a statute, regulation, or executive order, or in individualized discretionary use of nationality as a screening, investigation, or enforcement factor.

In order to ensure continued adherence to this policy, the DHS's Office for Civil Rights and Civil Liberties (CRCL), Privacy Office (PRIV), and Office of the General Counsel (OGC) will work with USCIS to conduct regular reviews of all ATLAS rules, keywords, and referral criteria to ensure that they are tailored to minimize the impact on individual civil rights, civil

[20] Janet Napolitano, "The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities" (Apr. 26, 2013). The Department of Justice issued "Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity" (December 2014), which supersedes the 2003 DOJ Guidance referenced in DHS policy.

liberties, and privacy and are in compliance with all threats relevant legal authorities, regulations, and DHS policies.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. Given that USCIS's CIV is a subset of a larger screening system, affecting a specific immigrant and nonimmigrant population of individuals, rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the FIPPs. This PIA examines the privacy impact of expanding the duration of CIV from the time of the initial immigrant or nonimmigrant benefit filing, through the duration of the benefit or status, until the individual becomes a naturalized U.S. Citizen.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

Privacy Risk: There is a risk that USCIS has not provided sufficient notice to inform an applicant or petitioner that the information he or she provides to USCIS will be subject to vetting under CIV, specifically that he or she is subject to vetting for the entire duration of his or her benefit unless and until he or she chooses to become a naturalized U.S. citizen.

Mitigation: This risk is mitigated because USCIS provides notice in several ways. First, USCIS provides notice to applicants and petitioners at the point of information collection through the Form Instructions for the application or petition benefit being filed. The Form Instructions ask applicants and petitioners to complete a set of eligibility standards to determine whether the individual is admissible and/or eligible to receive the benefit sought. The eligibility standards focus

on criminal acts and violations, including immigration violations and other unlawful activity. At the end of the application or petition, the applicant and/or petitioner is required to sign the form certifying that he or she authorizes USCIS to release any information received from the applicant or petitioner, as needed, to determine eligibility for benefits and when necessary for the administration and enforcement of U.S. immigration laws. In most cases, USCIS grants immigration benefits for a temporary period of time. During this status period, the applicant or petitioner is aware that the benefit is only for a certain time-period and subject to revocation, or unable to renew, if the applicant or petitioner becomes ineligible for the benefit due to not meeting the eligibility standards defined for the particular benefit.

Furthermore, certain forms, including the application to adjust to lawful permanent resident status, contain a statement on the Form Instructions that provides explicit notice that USCIS may verify information at *any time*, including before or after the individual's case is decided. This is consistent with CIV as an event-based screening initiative. This statement, referred to as the "USCIS Compliance Review and Monitoring" statement, provides notice that USCIS verification methods may include, but are not limited to: review of public records and information; contact via written correspondence, the Internet, facsimile, other electronic transmission, or telephone; unannounced physical site inspections of residences and locations of employment; and interviews. USCIS will use information obtained through verification to assess the applicant's compliance with the laws and to determine eligibility for an immigration benefit. Applicants and petitioners provide authorization and consent to USCIS completing these reviews before or after the benefit adjudication by signing and submitting the application or petition.

USCIS provides notice through the USCIS.gov[21] public website of the ways in which an individual can lose his or her status, including lawful permanent resident status, if the applicant or petitioner violates U.S. immigration laws.[22]

Finally, USCIS provides notice through the publication of this PIA and the related system PIAs. The PIA covering ATLAS, for example, describes the event-based vetting process, rules and production of SGNs, and the following events that trigger event-based vetting: 1) An individual presents him or herself to the agency (i.e., when USCIS receives an individual's application, such as for adjustment of status; when there is an update to an application; or when an applicant's fingerprints are taken at an authorized biometric capture site as part of the form application process); or 2) Derogatory information is associated with the individual in one or more Government databases.[23] The PIA also reflects the automated connection to ATS so that individuals are aware that ATS is a new source added to the existing event-based referral process.

---

[21] *See* https://www.uscis.gov/green-card/after-green-card-granted/maintaining-permanent-residence.
[22] Section 246(a) of the INA, 8 USC § 1256(a), and 212 and 237 of the INA.
[23] USCIS PIAs are available at www.dhs.gov/privacy.

CBP provides additional notice on the role ATS plays in assisting USCIS with CIV in an Addendum to its ATS PIA.[24]

Privacy Risk: There a risk that individuals are unaware that the information they submit will be shared with other systems/agencies.

Mitigation: This risk is mitigated. Applicants are required to sign the form certifying that he or she authorizes USCIS to release any information received from the applicant or petitioner, as needed, to determine eligibility for benefits and when necessary for the administration and enforcement of U.S. immigration laws. Furthermore, all USCIS forms contain a Privacy Act Statement or Privacy Notice that provides notice to individuals about the collection, USCIS's authority to collect information, the purposes of data collection, routine uses of the information, and the consequences of declining to provide the requested information to USCIS. Additionally, individuals receive general notice through this PIA.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Privacy Risk: There is a risk that an individual cannot consent to use of his or her information for CIV (i.e., vetting for the entire duration of his or her benefit unless and until he or she chooses to become a naturalized U.S. citizen).

Mitigation: During the adjudication process, individuals certify that they have not willfully misrepresented themselves or engaged in criminal activity. Engaging in these activities are grounds for denial or revocation. As stated above, most USCIS benefits are temporary in nature and subject to revocation or ineligible for renewal if the applicant or petitioner does not meet the immigration benefits eligibility standards. All individuals who apply or petition for immigration benefits with USCIS are required to submit and sign an application or petition authorizing the release of any information from their records that USCIS may need to determine their eligibility for the immigration benefit sought. By signing and submitting the form to USCIS, the applicant or petitioner consents to USCIS verifying such information and using the information to determine initial and continued eligibility. Certain USCIS forms also include a "Compliance Review and Monitoring" statement indicating that USCIS may verify information at *any time*, including before or after the case is decided. Furthermore, USCIS may require an individual to appear for an interview or provide fingerprints, photograph, and/or signature at any time to verify identity, obtain additional information, and conduct background and security checks, before making a decision on an application, petition, or request. Agency verification

[24] *See* DHS/CBP/PIA-006(b) Automated Targeting System (ATS) 2.4 Continuous Immigration Vetting Addendum, *available at* www.dhs.gov/privacy.

methods may include, but are not limited to: review of public records and information; contact via written correspondence, the Internet, facsimile, other electronic transmission, or telephone; unannounced physical site inspections of residences and locations of employment; and interviews.

Privacy Risk: There is a risk that individuals' options for redress may be limited if information obtained through CIV relates to national security information.

Mitigation: This risk is partially mitigated. To the greatest extent possible, USCIS provides individuals with opportunities to refute derogatory information throughout the adjudicative process. USCIS provides an applicant or petitioner 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). The applicant will have an opportunity to file motions or appeals if the application or petition is denied. Subject to the restrictions under 8 CFR 103.2(b)(16), USCIS will provide the applicant or petitioner an opportunity to address any adverse or derogatory information that may result from a USCIS compliance review, verification, or site visit after a formal decision is made on the case or after the agency has initiated an adverse action that may result in rescission or termination of the individual's status, including lawful permanent resident status.

USCIS continues to provide individuals with access to their information through a Privacy Act or Freedom of Information Act (FOIA) request. Both U.S. Citizens and Lawful Permanent Residents are eligible to file a Privacy Act request to access their information. Individuals not covered by the Privacy Act or Judicial Redress Act (JRA) still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record the request can be mailed to the following address:

National Records Center
Freedom of Information Act/Privacy Act Program
P. O. Box 648010
Lee's Summit, MO 64064-8010

Regardless of immigration status, FOIA does not afford an individual the right to amend his or her records. Should a non-U.S. person find inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

USCIS's authority is found in the INA, which specifies that the Secretary of Homeland Security has the authority to administer and enforce the INA[25] and may designate officers or employees to take and consider evidence concerning any matter that is material or relevant to the enforcement of the INA.[26]

In addition, 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, 8 U.S.C. §1103(a)(1), to administer the immigration laws (as defined in section 101(a)(17) of the INA).
>
> 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 Customs and Border Protection (CBP) or the CIS and make recommendations for prosecutions, or other appropriate action when deemed advisable."

USCIS has the authority to vet applicants for immigration benefits, before or after the adjudication, to determine whether national security concerns exist, or if there is other information that may impact the individual's right to remain in the United States (e.g., national security concerns, deportability concerns). Post-adjudication vetting allows USCIS to continue to enforce and administer the immigration laws by assisting in USCIS's ability to determine whether an individual obtained his or her status improperly or if the individual is potentially subject to rescission, termination, and/or to being placed in removal proceedings.

USCIS collects, retains, and shares information from applications, petitioners, beneficiaries, and other individuals connected to a benefit application or petition in accordance with a variety of System of Records Notices (SORN). The specific SORN is dependent on the population. However, the A-File, Index, and National File Tracking System,[27] Fraud Detection and National Security Records,[28] and Immigration Biometric and Background Check System[29] SORNs generally cover the use and maintenance of these records.

---

[25] 8 U.S.C. § 1103 (a)(1)
[26] 8 U.S.C. § 1357 (b)
[27] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).
[28] DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (Aug. 8, 2012).
[29] DHS/USCIS-018 Immigration Biometric and Background Check, 83 FR 36792 (July 31, 2018).

CBP's role is to act as a service provider for USCIS to assist in USCIS vetting of immigration benefit applicants. CBP is authorized to conduct this vetting pursuant to the authorities listed in the ATS[30] SORN.

Privacy Risk: There is a risk that use of information under this program will be inconsistent with the stated purpose and authorities.

Mitigation: This risk is mitigated. Filtering CBP vetting results through ATLAS's rules engine mitigates this risk in that ATLAS's rules are designed to produce information relevant to specific statutory provisions of the INA, such as Grounds for Inadmissibility[31] and Removable Aliens.[32] SGNs produced by ATLAS are required to be in compliance with the Privacy Act of 1974, E-Government Act of 2002, Homeland Security Act of 2002, and all DHS privacy policies and regulations. In order to comply with the privacy requirements, the DHS/USCIS/PIA-013(a) FDNS-DS Privacy Impact Assessment (PIA) was updated in May 2016 to include the use of screening Rules and Patterns and the SGN process and is continually updated to reflect updates to the system.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

Privacy Risk: To assist USCIS with immigration vetting, CBP will receive a greater volume of data on individuals applying for or receiving immigration benefits than CBP would otherwise receive when encountering these same individuals as part of its border security mission, thereby creating a risk of over-collection of information in ATS.

Mitigation: This risk is partially mitigated. USCIS has determined this volume of information is necessary to ensure the integrity of the ATLAS/ATS joint screening and matching capabilities. This information assists USCIS and CBP in validating the results and confirming a match to the individual (i.e., applicant/beneficiary). Further, retaining this data in ATS throughout the duration of the individual's status is necessary to enhance vetting capabilities in the event an individual presents themselves to DHS again, either through travel or in connection with immigration applications, petitions, or requests, or when derogatory information is added into Government databases due to investigations of or actions on behalf of the individual. The general requirement to purge the data from ATS when an individual naturalizes helps mitigate the risk of over-collection and any potential misuse of information. CBP will only access the data elements

[30] DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[31] 8 U.S.C. § 1182.
[32] 8 U.S.C. § 1227.

in these files if they are linked to a law enforcement or national security concerns.

Privacy Risk: There is also a risk of over-collection by USCIS. As CIV relies on connectivity to systems that have access to multiple databases, there is a risk of accessing and collecting more information than is relevant to determine an individual's eligibility to retain their status, including lawful permanent resident status.

Mitigation: This risk is mitigated. ATS connects with multiple data sources to complete its intended mission. However, for the purposes of this initiative, USCIS and CBP have narrowly tailored CIV to ensure that only relevant datasets are checked. Further, vetting results are filtered through ATLAS's event-based rules engine to tailor the results such that USCIS only receives automated notification of derogatory information that is consistent with pre-established indicators of national security concerns.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Privacy Risk: Expanding the duration of vetting under CIV will result in a longer period of retention of USCIS applicant data in ATS, thereby increasing the risk of secondary uses of data collected for the purpose of making determinations on eligibility for immigration benefits.

Mitigation: This risk is partially mitigated. CBP must retain this data in ATS in order to assist USCIS with vetting of certain immigrant applications for the full CIV vetting period. ATLAS has been configured to receive adjudication status updates and will deliver those updates to CBP ATS as notification of when an individual has naturalized and vetting should stop. CBP is required to return an acknowledgment of receipt of such notification as well as a "stopped CIV" indicator. With the exception of limited data, such as unique system identifiers, needed to support auditing capabilities, CBP will not retain this data in ATS after the issuance of the naturalization certificate unless the data is linked to active law enforcement lookout records, enforcement activities, or investigations or cases, in which case that data is maintained by CBP in ATS consistent with the ATS retention schedule as reflected in the ATS SORN (i.e., for the life of the law enforcement matter to support that activity and other enforcement activities that may become related). The limited data otherwise retained in ATS will be used solely for auditing purposes only, to support USCIS in its ability to conduct in depth quality reviews.

Privacy Risk: There is a risk that CBP may use the USCIS data for purposes other than CIV.

Mitigation: This risk is partially mitigated. CBP has agreed to only use the data for the purposes of CIV with the exception that CBP may use the data if it is linked to active law enforcement lookout records, enforcement activities, or investigations or cases. To enforce these

limitations, USCIS and CBP have entered into an Interagency Agreement that sets forth requirements associated with ongoing support of CIV, to include data use and retention. This agreement requires CBP to provide USCIS with a monthly progress report. In addition to the Interagency Agreement, USCIS and CBP routinely meet to discuss the CIV initiative and ensure the data exchanged is only used in support of the CIV initiative. Both USCIS and CBP have been actively involved in the drafting and publication of the PIA and are familiar with the limited uses set forth in this document. Both the PIA and established partnership between the Components keep the integrity of the program and ensure the uses are limited to only what was originally agreed upon.

Furthermore, USCIS and CBP program and oversight staff perform in-depth quality reviews of data exchanged under this program to ensure efficacy of the program, that the data is only used for the purpose for which it was originally intended, that data quality standards are met, and that the CIV process and exchange of information remains in compliance with approved governance standards, procedures, and privacy requirements. USCIS and CBP have dedicated privacy staff embedded in the program to assist with these reviews, to help with any necessary mitigation, and to support development of privacy compliance documents.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Privacy Risk: There is a general risk that information received through CIV will be inaccurate or incorrectly matched to an individual.

Mitigation: This risk is mitigated. USCIS has a vested interest and responsibility to maintain the most accurate data possible since the information could be used in support of an adjudicative decision or in support of criminal investigations undertaken by law enforcement partners. USCIS conducts manual reviews of all automated SGNs received under CIV to perform identity validation, confirm the validity of derogatory information, and to determine whether information is actionable. USCIS relies on multiple sources to confirm the veracity of the data and, if discrepancies are uncovered, will take necessary steps to correct inaccuracies.

Privacy Risk: In certain instances, the ATLAS and ATS systems may not receive accurate and timely updates as to an individual's immigration or citizenship status and will not stop vetting when an individual becomes a U.S. Citizen.

Mitigation: This risk is mitigated. USCIS has reviewed the immigrant and nonimmigrant population of individuals who would undergo CIV and designed the solution to incur the least possible risk. To ensure vetting does not occur on U.S. Citizens, USCIS has carefully scoped CIV so that it includes only individuals for which USCIS's systems have the technical capability to receive near real-time immigration status updates to relay to ATS, as an indicator of when an

individual has naturalized and vetting should stop. Additionally, USCIS has employed an internal quality controls and review process to evaluate technical performance, efficacy of the program, and to perform system tuning, when necessary, to ensure vetting results continue to be properly scoped throughout any expansion of CIV. Once ATLAS sends status updates to ATS, ATS returns confirmation of receipt and that vetting has stopped. This information is recorded in ATLAS and is auditable.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

This CIV process inherits all of the security and access controls established for the interconnected systems that support CIV. These are discussed in detail in the respective system PIAs. Strong access and security controls continue to mitigate privacy risks associated with authorized and unauthorized uses, specifically misuse and inappropriate dissemination of data.

ATLAS itself does not have a user interface. ATLAS pushes SGNs to FDNS-DS for FDNS officers' manual review. The FDNS-DS system has role-based access controls that ensure information is only accessed on a need-to-know basis, based on the users' current job functions and as verified by their supervisor and the FDNS-DS business owner. Only specially trained officers, known as gatekeepers, have access to review and triage SGNs in the FDNS-DS system and conduct reviews for validity before determining whether the SGN is actionable. This process is fully discussed in the FDNS-DS PIA.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

USCIS ensures that practices stated in this PIA comply with DHS and USCIS policies, including privacy policies, standard operating procedures, orientation and training, rules of behavior, and auditing and accountability. The systems that facilitate immigration vetting have robust auditing in place to enhance privacy and security by enabling senior leadership to be able to see whether information is being accessed and used appropriately and in accordance with all applicable information law and policy.

ATLAS auditing capabilities include: event processing logs to track the time of the event and a generic description of the event; user activity and session logging to track when a person has initiated a login session, including the time of the event and the login ID of the user signing onto the system; and a query/access log, which contains information specific to those systems that may have been accessed information via a service, including the time of the access, the login ID under

which the access occurred, the systems which were accessed, and systems that responded to the access request. This data is only accessible to IT Security and can be queried by login ID and time.

ATS auditing capabilities include: automated purge scripts to expunge records that have reached their retention limits; audit trails of information that has been entered into, sent from, and deleted from the system; and user roles that limit access to ATS data. These auditing tools will apply to all USCIS data sets in ATS and will facilitate compliance with retention and access limitations described in this PIA.

USCIS and CBP program and oversight staff perform in depth quality reviews of data exchanged under this program to ensure efficacy of the program, that data quality standards are met, and that the CIV process and exchange of information remains in compliance with approved governance standards, procedures, and privacy requirements. USCIS and CBP have dedicated privacy staff embedded in the program to assist with these reviews, to help with any necessary mitigation, and to support development of privacy compliance documents.

Further, employees who have access to records under this process receive system-specific training, annual privacy awareness, and security training, as well as specialized/on-the job training, and follow standard operating procedures that further reinforce privacy and security requirements.

Conclusion

USCIS remains committed to ensuring that immigration benefits are granted to individuals who do not pose a threat to national security or public safety, or who seek to procure an immigration benefit through the commission of fraud. CIV has many benefits, including earlier detection of information that may present national security concerns, identification of new or changed information, and immediate notification to USCIS when such information presents issues of national security that may impact an individual's eligibility for a benefit; application of uniform standards to screening and vetting of USCIS immigrant and nonimmigrant applications and petitions; and increased efficiencies in sharing of information among DHS partners with roles in enforcing immigration law. Recognizing these benefits come with potential risks, USCIS has thoroughly reviewed this process and taken steps to reduce the impact to individuals' civil rights, civil liberties, and privacy and to build in proper internal controls to evaluate the effectiveness and efficacy of the program. This allows USCIS to benefit from rapid detection and notification of risks to security of our nation while ensuring that only those individuals about whom there is a

known national security concern are impacted by the process. USCIS will continue to provide transparency through this PIA to account for any expansion and to evaluate privacy risks.

Responsible Officials

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

Approval Signature Page

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A:
INTERCONNECTED SYSTEMS THAT SUPPORT CIV

CBP Automated Targeting System (ATS): ATS is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments. For the purpose of this PIA, ATS is used to assist USCIS in vetting of immigration benefit applicants for national security.

USCIS ATLAS:[33] ATLAS is a USCIS platform that facilitates screening biographic and biometric information received from immigration benefit filings and uses rule-based computer automation to identify potential derogatory matches to records in DHS systems that indicate potential fraud, public safety, and national security concerns. When ATLAS detects a match to derogatory information, it produces System Generated Notifications (SGNs) to the FDNS case management system, Fraud Detection and National Security – Data System (FDNS-DS).

USCIS Fraud Detection National Security - Data System (FDNS-DS):[34] FDNS-DS is FDNS's primary case management system used to manage FDNS administrative investigations. SGNs are delivered to FDNS-DS as automated referrals of leads for FDNS review.

USCIS Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR):[35] ATLAS receives data associated with Form I-485 filings from Computer Linked Application Information Management System (CLAIMS 3) via eCISCOR.[36]

USCIS ELIS:[37] ATLAS receives data associated with Form N-400 filings from USCIS ELIS.

DHS IDENT:[38] ATLAS receives notifications from IDENT when a biometric encounter is matched to USCIS records. When IDENT returns biographic information that can be used to enhance the USCIS record, ATLAS will retrieve that information to be used for CIV.

---

[33] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS), *available at* www.dhs.gov/privacy.
[34] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS), *available at* www.dhs.gov/privacy.
[35] See DHS/USCIS/PIA-023(a) eCISCOR *available at* www.dhs.gov/privacy.
[36] See DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, *available at* www.dhs.gov/privacy.
[37] *See* DHS/USCIS/PIA-056 USCIS ELIS, *available* at www.dhs.gov/privacy.
[38] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.

APPENDIX B:
IMMIGRANT AND NONIMMIGRANT POPULATIONS (FORMS) TO BE VETTED UNDER CIV

Form Name	Population
Form N-400, *Application for Naturalization*	Applicant
Form I-485, *Application to Register Permanent Residence or Adjust Status*	Applicant