Privacy Impact Assessment

for the

ATLAS

DHS Reference No. DHS/USCIS/PIA-084

October 30, 2020

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) developed ATLAS (not an acronym) to automate, streamline, and support accurate exchange of data among USCIS, DHS, and non-DHS systems used to support biometric and biographic-based screening and vetting of immigration requests. ATLAS is used as both an automated check service platform and rule-based screening platform for USCIS. This Privacy Impact Assessment (PIA) evaluates the privacy risks and mitigations associated with ATLAS.

Overview

USCIS oversees many aspects of lawful immigration to the United States and is responsible for adjudicating applications, petitions, and other immigration-related requests (hereinafter collectively referred to as *immigration requests*)[1] while protecting the integrity of the U.S. immigration system. USCIS has a statutory obligation to ensure that an applicant and/or beneficiary is admissible in accordance with section 245(a)(2) of the Immigration and Nationality Act (INA).[2] Section 245(a)(2) requires that an alien must be admissible to the United States in order to adjust status to that of a lawful permanent resident (LPR). Section 212 of the INA lists several categories of inadmissible aliens.[3] An applicant may be found inadmissible, for example, if the applicant has been convicted of (or admits to having committed) an offense that constitutes a crime involving moral turpitude,[4] or has engaged in or is suspected of engaging in terrorist activities.[5] Similarly, section 237 of the INA[6] sets forth the grounds by which an alien can be determined to be removable or deportable, including a conviction for a crime involving moral turpitude[7] or security and related grounds.[8]

To ensure USCIS provides the right immigration benefit, to the right person, in the right amount of time, USCIS systematically conducts screening and vetting for every immigration request 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. USCIS conducts

[1] For purposes of this document, the term immigration request includes all benefit requests (as that term is defined in Title 8, C.F. R. Part 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.
[2] INA § 245(a)(2), 8 U.S.C. § 1255 ("Adjustment of status of non-immigrant to that of person admitted for permanent residence").
[3] *Id*. at § 212, 8 U.S.C. § 1255 ("Inadmissible aliens").
[4] *Id*. at § 212(a)(2), 8 U.S.C. § 1182(a)(2) ("Criminal and related grounds").
[5] *Id*. at § 212(a)(3), 8 U.S.C. § 1182(a)(3) ("Security and related grounds").
[6] *Id*. at § 237, 8 U.S.C. § 1227 ("General classes of deportable aliens").
[7] *Id*. at § 237(a)(2), 8 U.S.C. §1227(a)(2) ("Criminal offense").
[8] *Id*. at § 237(a)(4), 8 U.S.C. §1227(a)(4) ("Security and related grounds").

the following checks as part of screening and vetting processes:

Automated background checks: to obtain relevant information in order to render the appropriate adjudicative decision with respect to the benefit or service sought;

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.

In 2014, USCIS developed ATLAS[9] to automate, streamline, and support accurate exchange of data among USCIS and other Department, and non-DHS systems used to support biometric and biographic-based screening and vetting of immigration requests.[10] ATLAS is used as both an automated background check service and a rule-based screening platform for USCIS. In both capacities, ATLAS supports the screening and vetting of immigration requests related to applicants, beneficiaries, petitioners, sponsors, or other individuals associated with an immigration request.

ATLAS' automated background check and rule-based screening services enhance USCIS' vetting capability and strengthen USCIS' obligations under the INA by:

- Integrating screening and vetting capabilities with USCIS adjudicative case management systems;
- Increasing consistency and timeliness for automated background, identity, and security check operations;
- Detecting potential fraud, public safety, and national security concerns before, during, and after adjudicators begin reviewing immigration requests;
- Promptly notifying USCIS personnel with a role in the immigration screening and vetting process of information of potential concern meriting further analysis; and
- Ensuring consistent processes and procedures to operationalize screening and vetting enhancements.

[9] ATLAS was previously discussed in the PIA for the Fraud Detection and National Security – Data System. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE FRAUD DETECTION AND NATIONAL SECURITY DATA SYSTEM (FDNS-DS), DHS/USCIS/PIA-013(a) (2016), *available at* https://www.dhs.gov/uscis-pias-and-sorns. USCIS is separately working to remove the discussion of ATLAS from that PIA and reissue an updated version.
[10] *See* Appendix A for a full list of systems with connections to ATLAS.

ATLAS Automated Check Services

Historically, USCIS relied on manual point-in-time checks of various federal systems in order to accomplish the full suite of required background checks for a given immigration request.[11] Through the development of ATLAS, the need to independently query each system is greatly reduced, thereby streamlining the screening and vetting process. ATLAS serves as a conduit to transmit data between adjudicative case management systems and those systems used for background checks to perform certain automated background checks for immigration requests. As an automated check service, ATLAS is capable of performing:

- Automated ad-hoc checks, initiated by adjudicative case management system users; and
- Automated system-initiated checks on immigration requests processed in these systems.

ATLAS currently facilitates the U.S. Customs and Border Protection (CBP) TECS Name Check, which includes a check against the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) holdings, through TSSV,[12] for the majority of USCIS adjudication case management systems (e.g., USCIS Electronic Immigration System (USCIS ELIS),[13] CLAIMS 3,[14] and Global[15]). Through the Automated Check Service functionality, ATLAS may be used to provide and receive information from other interagency partners, either directly for unclassified information, or indirectly, for classified information. ATLAS' Automated Check

[11] During the adjudication process, USCIS conducts four different automated background checks, two biometric fingerprint-based, and two biographic name-based. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE IMMIGRATION BENEFITS BACKGROUND CHECK SYSTEM (IBBCS), DHS/USCIS/PIA-033 (2010), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021, (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ELECTRONIC IMMIGRATION SERVICE, DHS/USCIS/PIA-056 (2018 and subsequent updates), *available* at https://www.dhs.gov/uscis-pias-and-sorns.

[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3) AND ASSOCIATED SYSTEMS, DHS/USCIS/PIA-016 (2008 and subsequent updates), *available* at https://www.dhs.gov/uscis-pias-and-sorns.

[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ASYLUM DIVISION, DHS/USCIS/PIA-027 (2017 and subsequent updates) *available at* https://www.dhs.gov/uscis-pias-and-sorns.

Services may be subject to change or expand over time. A list of system connections and data sources is provided in Appendix A of this PIA.

Automated Background Check Results Review and Processing

ATLAS transmits results of system checks to adjudicative case management systems, consistent with established USCIS screening and vetting policies and procedures. Because ATLAS does not have a user interface of its own, the results of the automated background checks are available to USCIS adjudicators through the adjudicative case management systems (e.g., CLAIMS 3, USCIS ELIS). The results of the automated background checks are used by USCIS adjudication personnel to determine if the results impact eligibility for the benefit being sought. If the automated background check results indicate potential fraud, public safety, or national security concerns, the case is referred to Fraud Detection and National Security Directorate (FDNS) for administrative investigation and inputted into the FDNS-Data System (FDNS-DS).[16]

While USCIS has the legal authority to identify and investigate potential cases of national security, public safety, and fraud, USCIS may refer certain cases to the U.S. Immigrations and Customs Enforcement (ICE) for criminal investigation or enforcement action, as part of ICE's criminal investigative authority. Any follow-on action, to include the resolution of a System Generated Notification (SGN), further checks conducted, investigative processes, or referrals to ICE are recorded in FDNS-DS and the Alien File (A-File).[17]

ATLAS Rule-Based Screening

In addition to the automated background check service, ATLAS serves as a rules-based screening tool to screen immigration requests. ATLAS screens background and security check information and incorporates a range of automated processes for enhanced data correlation and screening - highlighting areas within a case requiring additional review. This information helps USCIS to:

- Detect potential threats earlier in the immigration benefit application process;
- Demonstrate the fidelity of the individual's biographic and biometric information; and
- Identify discrepancies more efficiently.

When an individual files an immigration request with USCIS, biographic data from the individual's form submission is captured in a USCIS adjudicative case management system (e.g., CLAIMS 3, USCIS ELIS, Global). For immigration requests that require biometric-based (e.g.,

[16] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE FRAUD DETECTION AND NATIONAL SECURITY DATA SYSTEM (FDNS-DS), DHS/USCIS/PIA-013 (2008 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[17] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (September 18, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.

fingerprint) checks, USCIS stores the biometrics that have been collected at Application Service Centers, at U.S. embassies, or by Refugee Officers in the field in the Customer Profile Management Service (CPMS)[18] and creates an encounter record in the DHS Automated Biometric Identification System (IDENT)[19] and the replacement Homeland Advanced Recognition Technology System (HART).[20]

ATLAS interfaces[21] with the aforementioned source systems to automatically receive data derived from the individual's immigration request or associated with individual biometric collection[22] or encounter records.[23] This data includes biographic identifiers such as name, date of birth, address, phone number, Alien Number, and receipt number. The exact data elements that ATLAS receives and transmits during automated screening varies depending on the type of immigration request, what data is captured in the source system, and what data elements are needed to perform required automated background checks.

ATLAS compares information in the immigration request against criminal, customs, immigration, and counterterrorism information held in government systems, using rule-based computer automation, rather than manual system checks, to automate identification of potential derogatory information that matches to information in the immigration request. ATLAS interfaces with a number of USCIS and DHS systems in order to receive and transmit data associated with screening and vetting processes.

A complete list of system connections and data sources that support ATLAS screening is provided in Appendix A of this PIA.

The immigration request information and the associated automated background check results filter through a predefined set of rules to determine whether the information provided by the individual or obtained through the required checks presents a potential fraud, public safety, or

---

[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CUSTOMER PROFILE MANAGEMENT SERVICE, DHS/USCIS/PIA-060 (2015 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[19] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-002 (2012) *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[20] *See* U U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[21] ATLAS interfaces with systems both through direct connections and through connections to other USCIS services/microservices that transmit data to/from USCIS and DHS systems. A complete list of system interfaces is provided in Appendix A.

[22] ATLAS does not receive the individual's biometrics, but receives biographic identifiers linked to the individual's biometric capture or encounter record, such as Fingerprint Identification Number (FIN), Encounter Identification Number (EIN), or Organization/Unit/Sub-Unit (OUS) code of the organization that generated an encounter record in IDENT.

[23] Each time an individual's biometrics are enrolled in DHS IDENT, it is referred to as an encounter.

national security concern. The automated rules help standardize how information is analyzed and help to detect patterns, trends, and risks related to fraud detection, public safety, national security, and admissibility issues that are not easily apparent from the immigration request submissions themselves.

This automated rule-based screening capability is event-based, meaning it is triggered by the occurrence of an event. Therefore, some ATLAS rules screen on a recurring basis as events occur, including when:

- An individual presents him or herself to the agency (*e.g.*, when USCIS receives an individual's immigration request[24] or while collecting an individual's fingerprints at an authorized biometric collection site, for those immigration requests that require biometric checks); or
- New derogatory information[25] is associated with the individual in one or more U.S. Government systems.[26]

Continuous Immigration Vetting (CIV) is a specific type of rule-based screening that ATLAS facilitates. To provide additional transparency into CIV, USCIS issued DHS/USCIS/PIA-076 Continuous Immigration Vetting.[27]

Review and Processing

If the rule criteria are met, an automated SGN is transmitted to FDNS-DS, for manual review by a specially trained officer or analyst, known as a Gatekeeper.[28] The Gatekeeper verifies whether the information relates to the applicant and determines whether the SGN is actionable. An SGN found not to relate to an applicant or to be unactionable may be closed without further action or after the Gatekeeper has taken corrective action to resolve data integrity concerns.

If the SGN is actionable, FDNS initiates an administrative investigation[29] by following the FDNS-DS case management process, as described in the FDNS Directorate PIA.[30] In accordance with standard FDNS processes, when an SGN results in a FDNS administrative investigation and

[24] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE BENEFIT REQUEST INTAKE PROCESS, DHS/USCIS/PIA-061 (2020), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[25] Derogatory information is information which potentially has an unfavorable impact on the adjudication of an immigration request.
[26] This may occur before or after the adjudication of the immigration request.
[27] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CONTINUOUS IMMIGRATION VETTING, DHS/USCIS/PIA-076 (2019), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[28] *See supra* note 16.
[29] FDNS administrative investigation functions related to national security or public safety may also be performed by Background Check Unit personnel.
[30] *See supra* note 9.

information related to the investigation needs to be shared with adjudications personnel, FDNS personnel memorializes the relevant information through official documentation such as a Statement of Findings (SOF). Manually reviewed information found in the rule-based ATLAS screening process may be used to inform eligibility determinations, which will result in the approval or denial of a benefit.

As discussed above, USCIS may refer potential cases of national security, public safety, and fraud to ICE for criminal investigation or enforcement action. All follow-on action from ICE and external partners is recorded in FDNS-DS, to the extent possible.

Governance and Oversight

USCIS has established a formal governance structure to ensure that ATLAS screening rules are compliant with all legal, policy, privacy, and civil rights and civil liberties requirements. New rules undergo operational, legal, privacy, and policy review before they are presented to USCIS executive leadership for final approval. As a new rule is conceived, whether it be to detect national security and public safety threats, fraud indicators, or inadmissibility patterns, the governance structure carefully considers legal, privacy, policy, and operational requirements in developing the rule criteria. USCIS executive leadership considers this information when approving and/or prioritizing development of ATLAS screening rules.

Through this process, USCIS ensures that all screening activity is properly vetted and falls within USCIS' authority. All screening methods deployed are tailored to provide information that is relevant to statutory grounds of inadmissibility[31] or deportability[32] found in the INA or that may affect an individual's eligibility for a benefit. USCIS may conduct screening and vetting in situations in which USCIS has the authority to rescind, revoke, or otherwise terminate a benefit; to issue a Notice to Appear (NTA);[33] 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. § 1367 and other immigration specific confidentiality provisions.

After leadership approval is given, USCIS begins technical implementation and conducts testing, prior to deployment. USCIS preforms testing within various technical staging environments, where the performance of functions is evaluated, system issues are resolved, and any indicated improvements in system design or operation are addressed. USCIS also conducts testing to measure match errors and select thresholds and configure business rules (i.e., how the system implements sharing and restrictions in accordance with applicable agreements) to reduce

[31] *Id*. at § 212, 8 U.S.C. § 1255 ("Inadmissible aliens").
[32] *Id*. at § 237, 8 U.S.C. § 1227 ("General classes of deportable aliens").
[33] USCIS has authority to issue Form I-862, *Notice to Appear*, which is thereafter filed with the Immigration Court to commence removal proceedings under section 240 of the INA. See, e.g., INA §§ 103(a), 239; Title, 8 C.F.R. Parts 2.1, 239.1.

error rates. Any issue identified is resolved and retested prior to deployment approval to ensure the rule and pattern criteria are working as designed, and expected SGNs are alerting effectively.

USCIS is committed to the fair and equal treatment of all individuals in the screening and vetting activities, ensuring the rights of all people while taking lawful actions necessary to protect the integrity of the legal immigration system. 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. This includes prohibiting the consideration of race or ethnicity in investigation, screening, and law enforcement activities in all but the most exceptional instances and limiting the consideration of an individual's simple connection to a particular country, by birth or citizenship, as a screening criterion, unless 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, citizenship, or nationality.[34]

Compliance and Data Quality Reviews

To ensure continued adherence to this DHS policy, USCIS works through its structured governance process to review ATLAS rules, keywords, and referral criteria so that they are tailored to minimize the impact on individual privacy, civil rights, and civil liberties and are in compliance with all relevant legal authorities, regulations, and DHS policies. USCIS coordinates with the DHS Privacy Office (PRIV), Office for Civil Rights and Civil Liberties (CRCL), Office of the General Counsel (OGC), and the Office of Strategy, Policy, and Plans for each of these reviews.

FDNS performs compliance reviews on data captured through ATLAS processes and FDNS-DS and produces analyses to identify and develop information on fraud indicators, patterns, and trends.[35] These analyses include considerations to preserve the privacy and civil rights/civil liberties of all individuals who undergo screening and vetting. The same commitment is used to design, build, and maintain ATLAS in a manner that poses the least possible impact on individuals' privacy civil rights, and civil liberties.

FDNS performs data quality reviews on data streaming through ATLAS for system screening and vetting (i.e., background, identity, and security checks) to ensure compliance with

[34] Janet Napolitano, U.S. DEPARTMENT OF HOMELAND SECURITY, MEMORANDUM FOR COMPONENT HEADS, THE DEPARTMENT OF HOMELAND SECURITY'S COMMITMENT TO NONDISCRIMINATORY LAW ENFORCEMENT AND SCREENING ACTIVITIES, (April 26, 2013), *available at* https://www.dhs.gov/sites/default/files/publications/secretary-memo-race-neutrality-2013_0_1.pdf; U.S. DEPARTMENT OF JUSTICE, GUIDANCE FOR FEDERAL LAW ENFORCEMENT AGENCIES REGARDING THE USE OF RACE, ETHNICITY, GENDER, NATIONAL ORIGIN, SEXUAL ORIENTATION, OR GENDER IDENTITY, (December 2014), *available at* https://www.justice.gov/sites/default/files/ag/pages/attachments/2014/12/08/use-of-race-policy.pdf, which supersedes the 2003 DOJ Guidance referenced in DHS policy.

[35] *See supra* note 16.

USCIS screening policy, legal, and privacy requirements and to validate that the technical design works as intended and as approved by the governance structure. Additionally, FDNS performs data quality reviews on SGNs within the FDNS-DS. SGNs are routinely and randomly reviewed by ATLAS Screening and Analysis officers to ensure the defined screening criteria are met, the SGNs are operating as designed, and the proper triaging is occurring according to the SGN Gatekeeping User Guides. Additionally, every automatically-generated match, or "hit," is reviewed by a specially-trained officer or an analyst (Gatekeeper) to verify that the match is valid and to determine whether the information appears to be actionable. If it does, then the information contained in the SGN will enter the formal FDNS case management process maintained in FDNS-DS, according to established processes, for action by an FDNS Officer and/or Background Check Unit personnel.

Routinely, FDNS produces and analyzes SGN reporting, which aids in data quality reviews. Several layers of FDNS personnel review this reporting for authenticity and accuracy. This provides an accounting for pending triage workloads, work achieved, and adjustments in triaging practices. The ATLAS Screening and Analytics Team also performs SGN quality reviews, to include reviewing how the SGN fired (or "alerted"), if it fired as the system was designed, and to analyze for any improvements that can be made. For certain SGN populations, this is performed on a monthly basis. For others, the checks are performed at random and ad-hoc.

Privacy Impact Assessment

USCIS first published notice of ATLAS as part of the FDNS-DS PIA, as a means to discuss the automatic referrals of SGNs. ATLAS now serves as a hub within USCIS to facilitate screening and vetting across multiple platforms, transmitting a significant amount of personally identifiable information (PII), and thus, USCIS is issuing a new PIA to evaluate the privacy risks associated with ATLAS.

This PIA covers and discusses the privacy risks and mitigation strategies associated with ATLAS' screening capabilities and services. A separate PIA was published February 14, 2019, to discuss CIV in more depth, to include privacy risks and mitigation strategies specific to vetting identified immigrant and non-immigrant requests for the duration of their status, until naturalization.[36]

The privacy risks and mitigation strategies associated with the overall administrative investigation process and case management system are described in the FDNS Directorate PIA and FDNS-DS PIA. Additionally, other published USCIS PIAs available at https://www.dhs.gov/uscis-pias-and-sorns cover the benefit request intake process, benefit request form analysis, and case management systems and processes, as well as the collection of biographic and biometric information that is used as part of the screening and vetting process. These published

[36] *See supra* note 27.

PIAs provide an in-depth discussion of these separate processes and evaluate the privacy risks and mitigation strategies built into each process.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The legal authority to collect this information comes from the Immigration and Nationality Act, 8 U.S.C. Section 1101, *et seq*. 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 (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] and make recommendations for prosecutions, or other appropriate action when deemed advisable.[37]

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

ATLAS enables real-time information sharing between USCIS and DHS IT systems. While ATLAS does not retrieve information by personal identifier, the following source system SORNs cover the collection, use, maintenance, and dissemination of information in support of the automated background check service and rule-based screening platforms:

- Alien File, Index, and National File Tracking SORN covers maintenance of records in the A-File.[38]
- Asylum Information and Pre-Screening SORN covers data collected from requests for asylum status.[39]

[37] Initially named "Bureau of Citizenship and Immigration," or BCIS, the agency was quickly renamed U.S. Citizenship and Immigration Services (USCIS).
[38] *See supra* note 17.
[39] *See* DHS/USCIS-010 Asylum Information and Pre-Screening, 80 Fed. Reg. 74781 (November 30, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.

- Benefits Information System SORN covers data collected from USCIS immigration requests, other than requests for refugee or asylum status.[40]
- Immigration Biometric and Background Check (IBBC) SORN covers the collection, use, and storage of biometric and biographic data for background checks and its results, covers background checks and their results.[41]
- Intercountry Adoptions SORN covers the collection of information during the intercountry adoptions process.[42]
- Fraud Detection and National Security Records (FDNS) SORN covers maintenance of records in FDNS-DS and other FDNS records.[43]
- Refugee Case Processing and Security Screening Information SORN covers the collection, use, maintenance, and dissemination of refugee data, to include application intake, security checks, and adjudication.[44]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. ATLAS is a capability associated with the FDNS-DS system, which was approved for entrance into the DHS Ongoing Authorization (OA) Program on August 26, 2014. OA requires ATLAS to be reviewed by the USCIS OA Team on a monthly basis and maintain its security and privacy posture to maintain its Authority to Operate (ATO). ATLAS is included in the FDNS-DS system privacy plan.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

ATLAS only maintains audit and transactional logs of all data sent and received in accordance with General Records Schedule DAA-GRS2013-0006-0003, which states that the records are destroyed when the business use ceases.

ATLAS' SGNs are transmitted to the FDNS-DS system and are maintained in accordance with the NARA-approved FDNS-DS retention schedule, N1-566-08-18. Under this retention

[40] *See* DHS/USCIS-007 Benefits Information System, 84 Fed. Reg. 54622 (October 10, 2019), *available at* https://www.dhs.gov/system-records-notices-sorns.
[41] *See* DHS/USCIS-018 Immigration Biometric and Background Check (IBBC), 83 Fed. Reg. 36950 (July 31, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[42] *See* DHS/USCIS-005 Inter-Country Adoptions Security, 81 Fed. Reg. 78614 (November 8, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[43] *See* DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 Fed. Reg. 47411 (August 8, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[44] *See* DHS/USCIS-017 Refugee Case Processing and Security Screening Information, 81 Fed. Reg. 72075 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

schedule, FDNS-DS retains records 15 years from the date of the last interaction between FDNS personnel and the individual. Records related to an individual's A-File are be transferred to the A-File and maintained under the A-File retention period. This includes USCIS IT systems containing electronic A-File content.

Records transmitted to USCIS adjudicative case management systems are retained electronically in those systems according to their respective retention schedules.

USCIS retains full screening and vetting results for 100 years from the date of birth of the immigration requestor in accordance with NARA Disposition Authority Number DAA-0563-2013-0001-0005. The 100-year retention rate comes from the length of time USCIS may interact with an immigration requestor. Further, retaining the data for this period of time will enable USCIS to identify fraud and misappropriation of benefits.

USCIS maintains records on individuals and all of their immigration transactions and law enforcement and national security actions (if applicable), in the A-File. A-File records are permanent records in both electronic and paper form. USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth, in accordance with N1-566-08-011.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Almost all of the information within ATLAS is originally submitted on an immigration request form that is subject to the PRA. However, there are no forms associated specifically with the collection of information in ATLAS. Please see the benefit request PIAs and Appendices for a comprehensive list of the various forms that cover the initial collection of information from the individual.[45]

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

ATLAS collects information on individuals from all immigration requests. This may include information on the applicant, beneficiary, petitioner, sponsor, and/or other individuals associated with the immigration request. The exact data elements that ATLAS receives and

[45] For example, DHS/USCIS/PIA-061 BENEFIT REQUEST INTAKE PROCESS (*supra* note 24).

transmits will vary depending on the type of immigration request, what data is captured and available in the source system, and what data elements are needed to perform required checks, and what data elements are required to transmit the available vetting results.

ATLAS sends information derived from the individual's immigration request or biometric collection to be screened against U.S. Government systems that contains information about law enforcement, public safety, or national security threats. In the event of a match, ATLAS receives the results and transmits the results to the appropriate USCIS adjudicative case management system and/or to FDNS-DS through SGNs for USCIS personnel to review.

2.2 What are the sources of the information and how is the information collected for the project?

ATLAS collects information throughout the screening and vetting (i.e., background, identity, and security check) process. Much of the information collected by ATLAS is derived from an immigration request submitted to USCIS by the individual or an authorized representative or preparer, or from the individual's biometric collection at an authorized biometric collection site, as part of the immigration request/application process. ATLAS also collects information from other governmental systems which is used as part of the screening and vetting process.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. ATLAS does not collect or use information from commercial or public sources.

2.4 Discuss how accuracy of the data is ensured.

ATLAS relies on the accuracy of the information as it is collected from the immigration requestor and from the other government source systems. As such, the accuracy of the information in ATLAS is equivalent to the accuracy of the source information at the point in time when it is collected by ATLAS.

Manual review is built into all USCIS screening and vetting processes such that USCIS personnel review all results and perform data validation through review of the underlying immigration request, or by verifying information with the individual through in-person interviews

or issuing Requests for Evidence (RFE)[46] or Notices of Intent to Deny (NOID).[47] This process ensures information is matched to the correct individual, as well as integrity of the data.

If USCIS learns of inaccurate information obtained through ATLAS, USCIS personnel will contact the record owner or source system to seek modification or correction of the record.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that USCIS will obtain and rely upon inaccurate data.

Mitigation: The 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 or national security investigations undertaken by law enforcement or intelligence partners. USCIS collects much of the information directly from the immigration requestor. USCIS presumes the information submitted is accurate and verifies the information against multiple sources during the review process. USCIS gives the immigration requestor multiple opportunities during and after the completion of the application process to correct information he or she has provided and to respond to information received from other sources. If the information could lead to a denial of the immigration request and if it is information of which the applicant is unaware, it would be provided to the immigration requestor in a NOID, in an interview, or in similar processes, and the immigration requestor would have an opportunity to review and respond.

Information not collected directly from the immigration requestor is collected from government systems. USCIS relies upon the accuracy of information as it is collected in those systems. As such, the accuracy of information collected and transmitted by ATLAS is equivalent to that of the source system.

Manual review is built into all USCIS processes that rely upon data from ATLAS to verify accuracy of information, to include determining its validity and whether or not the information is actionable, within USCIS' authorities. Data validation includes manual reviews of information in the underlying immigration requests, performing additional system checks, or contacting the record owner to verify information, or verifying information with the individual through in-person interviews, issuing RFEs or NTAs, or through other administrative processes, to ensure

[46] USCIS uses an RFE when an application lacks required documentation, or the adjudicator needs additional evidence to determine an applicant's eligibility for the benefit sought. The request will indicate what evidence or information USCIS needs to fully evaluate the application or petition under review.
[47] A NOID is a formal statement from USCIS that it has determined that the applicant is ineligible for the immigrant benefit requested. The issuance of a NOID is required when derogatory information is uncovered during the course of the adjudication that is not known to the individual, according to Title 8, C.F.R. Part 103.2(b)(16). However, USCIS will grant the applicant an opportunity to overcome this determination and demonstrate that he or she is eligible.

information is matched to the correct individual. In the event USCIS learns of inaccurate information, USCIS personnel will contact the record owner or source system to seek correction of the record.

Additionally, data quality is an important consideration during the governance process in determining new data sets for ATLAS. After deployment, FDNS performs routine and ad-hoc SGN reporting and compliance and data quality reviews. Dedicated USCIS personnel are responsible for performing SGN quality reviews, including the need for additional trainings and rule refinements. These reviews ensure ATLAS rules and SGNs are alerting as intended and producing information that is accurate, timely, and relevant to evaluating the underlying immigration request.

Privacy Risk: Because ATLAS aggregates information from multiple source systems, there is a risk of data inaccuracy if the data in the underlying system(s) changes.

Mitigation: This risk is mitigated. ATLAS collects information from the source systems in near real-time; therefore, the information collected and transmitted by ATLAS is equivalent to the accuracy of the source information at the point in time when it is collected by ATLAS. Additionally, the manual review process ensures USCIS relies on the best possible data in making determinations that relate to individuals.

Privacy Risk: There is a risk that ATLAS has access to more data than is necessary to perform the automated background check service and rules-based screening.

Mitigation: This risk is mitigated. ATLAS itself does not have a user interface. ATLAS transmits automated background check results and SGNs to USCIS adjudicative case management systems and FDNS-DS, respectively, for USCIS personnel to review. All USCIS adjudicative case management systems and FDNS-DS have role-based access controls that ensure information is only accessed on a need-to-know basis and based on the users' current job functions and as verified by their supervisor and the system business owner. Additionally, only specially trained officers, known as Gatekeepers, have access to review and triage SGNs and conduct reviews for validity before determining whether the SGN is actionable. Lastly, USCIS has a robust governance process, which ensures that ATLAS screening is appropriately tailored to specific, identified criteria that has been reviewed for legal, privacy, policy, civil rights and civil liberties, and operational considerations. The governance structure ensures that all ATLAS screening rules are compliant with identified requirements and that all screening activity is properly vetted and falls within USCIS' authority, to include delivering information to the end users that is relevant to the specific screening and vetting request.

Privacy Risk: There is a risk of obtaining data from new sources that have not been reviewed for privacy and legal concerns in determining possible benefit fraud, criminal activity, public safety, and national security concerns.

Mitigation: This risk is mitigated. Through the governance process, all new data sources undergo legal, privacy, policy, and operational review and are approved by USCIS executive leadership prior to deployment. This includes ensuring new data collected falls within the scope of USCIS' authority and is covered in USCIS' published SORNs.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

USCIS uses ATLAS as both an automated background check service platform and rule-based screening platform. As an automated background check service, ATLAS receives information from the individual's immigration request form and serves as a conduit to transmit information needed to perform the required automated background, identity, and security checks and returns the results of the checks to the respective adjudicative case management systems. As a rule-based screening platform, ATLAS receives the immigration request form and automated background check result information described above and filters it through a predefined set of rules to determine whether the information presents a potential fraud, public safety, or national security concern. If the rule criteria are met, an automated SGN is sent to FDNS-DS to alert a Gatekeeper of the potential derogatory information. The Gatekeeper is responsible for manually reviewing the information to verify whether the information relates to the applicant, and whether the SGN is actionable.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. ATLAS contains a rules engine that applies pattern-based algorithms to look for indicators of fraud, public safety, and national security concerns. Through this process, ATLAS is able to discover potentially derogatory information based on pre-defined criteria, and to generate SGNs to systematically refer cases of potential concern to FDNS-DS for further review by a Gatekeeper.

An SGN in itself is not considered derogatory. SGNs merely serve as alerts that review of potential concerns is warranted. Gatekeepers review SGNs and perform data validation through

review of the underlying immigration request, conducting additional checks of government systems and/or by verifying information within the A-File(s). When a Gatekeeper has performed manual review and validation and confirmed information is actionable, that information enters the formal FDNS case management process maintained in FDNS-DS.

As described above, confirmed derogatory information that is actionable may result in an FDNS administrative investigation and may also be referred to ICE for criminal action. Once FDNS concludes its review or administrative investigation, findings are provided to USCIS adjudicative personnel to assist in informing an adjudicative decision. This information is ultimately placed in the individual's A-File record.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. ATLAS does not have a user interface, and therefore, there are no end-users with roles within the ATLAS system itself. However, results of screening and vetting can be viewed by other DHS components who have access to systems to which ATLAS transmits data. For example, ATLAS transmits automated background, identity, and security check requests from case management systems to other federal systems to facilitate required screening and vetting. ATLAS then sends screening and vetting results to USCIS adjudicative case management systems where adjudications of immigration requests are managed, as well as FDNS-DS. Other DHS components, such as ICE and CBP, have access to adjudicative case management systems, and may access automated background check results generated by ATLAS. Additionally, the responses may have generated SGNs in FDNS-DS where FDNS investigations are managed.

ATLAS SGNs may only be triaged in FDNS-DS by USCIS personnel who have a Gatekeeper role in the FDNS-DS system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information collected and transmitted by ATLAS may be used inappropriately or not in accordance with the original collection purpose or associated authorities.

Mitigation: This risk is mitigated. USCIS has created a governance process, which requires a full legal, privacy, policy, and operational review for ATLAS screening and rules pre-deployment, as well as the post-deployment compliance, data quality, and oversight reviews that confirm screening remains compliant, appropriately tailored, and relevant to current concerns or threats. Use of the information is designed to be consistent with existing USCIS screening and vetting, investigative, and adjudicative policies and procedures.

ATLAS transmits results of system checks to USCIS adjudicative case management systems, consistent with established USCIS screening and vetting policies and procedures. End users who view the results from within the respective adjudicative case management systems will only receive and use information which they are authorized to receive. ATLAS' rules-based detections of fraud, public safety, and national security concerns are designed specifically to generate automated referrals, through SGNs, to FDNS-DS. This ensures information is properly evaluated by specially trained Gatekeepers to determine if the information yields potential fraud or a risk to public safety or national security and may impact an individual's eligibility for an immigration benefit. ATLAS' rules also minimize transmission of PII by filtering screening and vetting results to return only information that meets pre-defined patterns of fraudulent or nefarious activity.

Privacy Risk: There is a risk that SGNs may present Gatekeepers with results that may contain too many false positives, which may render the resulting data unusable or unreliable or unfairly subject individuals to further scrutiny.

Mitigation: This risk is mitigated. As SGNs are conceived, USCIS captures requirements and potential criteria for an SGN from end users (e.g., USCIS adjudicators and officers) and works closely with the governance entities to carefully select criteria to reduce false positives and focus on detection of potential national security, public safety, and fraud indicators, leveraging from information within the various connected systems.

Once the criteria are established and development is complete, a testing phase allows for a period of refining rules, if needed, before they are deployed across FDNS. This is performed in a testing environment, before deployment into the live production environment where SGNs are created and sent to FDNS-DS. The members of this testing team include system experts, as well as FDNS personnel. This initial effort minimizes the risk of false positive SGNs. Once sufficiently refined, the SGN is deployed.

The SGN triage process provides a layer of human review to confirm SGNs are actionable prior to routing them for further case management activity within FDNS-DS. Between the systematic and human processes, FDNS will identify any needed enhancements. SGN criteria can then be modified or enhanced to better detect actionable, derogatory information.

Privacy Risk: There is a risk that screening and vetting results and data may be taken out of context by the end users who view results in the USCIS adjudicative case management systems.

Mitigation: This risk is mitigated. ATLAS provides baseline automated background, identity, and security check results to USCIS adjudicative case management systems in the form of a "hit" or "no hit" response or a summary of past screening and vetting history, which indicates which checks were completed and when. The responses sent to the case management systems are tailored to present adjudication officers with information relevant to determining the immigration

requestor's eligibility for the benefit or service sought. However, to gain a full understanding of the screening and vetting results, and to specifically review any derogatory information, users must review the Alien File, including all prior security check results.

Privacy Risk: There is a risk that ATLAS will be used to screen and vet individuals for longer than necessary.

Mitigation: This risk is mitigated. USCIS has a number of mechanisms in place to ensure ATLAS screening remains within its authorized and stated purposes, to include the ATLAS governance process, the ATLAS Screening and Analytics compliance and data quality reviews, and continued oversight involvement. Through these processes, USCIS considers the appropriate length of time to perform automated screening and rules-based detections for fraud, public safety, and national security concerns. USCIS performs reviews to ensure SGNs are alerting within the appropriate timeframes 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.

However, USCIS has the authority to vet applicants for immigration benefits, before or after the adjudication and 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). USCIS established a specific program, known as CIV, to allow for post-adjudication vetting and notification, when new information is discovered in U.S. Government systems that relates to an individual's immigration request. USCIS published a separate PIA to provide transparency into how this process impacts individuals who apply for benefits with USCIS and to discuss the privacy risks and mitigations associated with CIV.

Privacy Risk: There is a risk that FDNS will create ATLAS rules without going through the appropriate rules review process.

Mitigation: This risk is mitigated. The governance process ensures that new rules are not created or implemented without review from the appropriate stakeholders, including privacy and legal review. Implementation of rules and generation of SGNs are required to be in compliance with the Privacy Act of 1974,[48] E-Government Act of 2002,[49] Homeland Security Act of 2002,[50] and all DHS privacy policies and procedures. Additionally, the capture, use, and disclosure of PII through the rules process must be pursuant to applicable SORNs and available routine uses.

Privacy Risk: There is a risk that USCIS may not appropriately protect special protected class data (e.g., 8 U.S.C. § 1367 VAWA, U, and T visa applicants) information in ATLAS.

[48] 5 U.S.C. § 552a.
[49] 44 U.S.C. § 3501 note.
[50] 6 U.S.C. § 142.

Mitigation: This risk is partially mitigated. USCIS generally uses only the combination of name and date of birth to conduct an automated background check. Special protected class information is typically not tagged in ATLAS. However, as described above, because ATLAS does not have a user interface, the results are displayed either in a USCIS adjudicative case management system (e.g., CLAIMS 3) or via FDNS-DS as an SGN. USCIS places the responsibility on the interconnected system to tag protected data, or to display information indicating that an individual is a protected class.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

USCIS provides notice to applicants and petitioners at the point of information collection through the Form Instructions for the application, petition, or other request 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.

All forms have a Privacy Notice providing notice to the individual regarding the use and collection of the information and that information may be used for fraud, law enforcement, or national security detection. USCIS forms also notify the individual that information provided may be checked for completeness, that certain background checks may be conducted, or that USCIS may request an interview or further evidence. In most cases, USCIS grants immigration benefits for a temporary period of time.[51] 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 may not be renewable, if the applicant or petitioner becomes ineligible for the benefit due to not meeting the eligibility standards defined for the particular benefit.

[51] Adjudicators are responsible for making decisions regarding granting benefits.

USCIS also provides notice of USCIS policies and procedures though the USCIS public website.[52] Finally, USCIS provides notice through the publication of this PIA and the related USCIS PIAs and SORNs, as previously referenced.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

USCIS provides individuals seeking USCIS benefits with a Privacy Notice contained on all immigration request form instructions. The Privacy Notice details the legal authority for the collection of the information requested and the uses of information. As a general rule, USCIS provides notice that the information collection is voluntary, and that the individual may decline to provide the requested information. However, failure to provide the requested information may delay a final decision or result in the denial of the applicant's immigration request. On each immigration request form, USCIS includes a release authorization statement that requests the applicant's signature to permit USCIS to release any information from the applicant's records necessary to determine eligibility for the requested benefit.

Further, fraud assessments and background, identity, and security checks are required by regulation on all immigration requests filed with USCIS. Immigration requests cannot be granted until those checks are complete. The information supplied on the immigration request form is essential to conduct those checks.[53]

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that USCIS has not provided sufficient notice for individuals to understand how ATLAS collects and shares information as part of the screening and vetting (*i.e.*, automated background, identity, and security check) process.

Mitigation: This risk is mitigated. USCIS provides notice to individuals through form instructions, Privacy Notices, the source system PIAs, the FDNS Directorate PIA, the CIV PIA, this PIA, and the associated SORNs. USCIS also provides notice of its fraud detection and national security work through its public website.[54]

---

[52] *See* https://www.uscis.gov/.
[53] As required by 8 U.S.C. § 1101, et seq.
[54] *See* https://www.uscis.gov/about-us/directorates-and-program-offices/fraud-detection-and-national-security/fraud-detection-and-national-security-directorate.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

ATLAS only maintains audit and transactional logs of all data sent and received. ATLAS retains audit logs associated with this service in accordance with General Records Schedule DAA-GRS2013-0006-0003, which states that the records are destroyed when the business use ceases.

ATLAS' SGNs are transmitted to the FDNS-DS system and are maintained in accordance with the NARA-approved FDNS-DS retention schedule, N1-566-08-18. Under this retention schedule, FDNS-DS retains records 15 years from the date of the last interaction between FDNS personnel and the individual. Per procedure, FDNS findings related to an individual's A-File are transferred to the A-File and maintained under the A-File retention period. Records transmitted to USCIS adjudicative case management systems are retained electronically in those systems according to their respective retention schedules.

USCIS retains full screening and vetting results for 100 years from the date of birth of the immigration requestor in accordance with NARA Disposition Authority Number DAA-0563-2013-0001-0005. The 100-year retention rate comes from the length of time USCIS may interact with an immigration requestor. Further, retaining the data for this period of time will enable USCIS to identity fraud and misappropriation of benefits.

USCIS maintains records on individuals and all of their immigration transactions and law enforcement and national security actions (if applicable), in the A-File. A-File records are permanent records in both electronic and paper form. USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth, in accordance with N1-566-08-011.

5.2 Privacy Impact Analysis: Related to Retention

There is no risk related to data retention because ATLAS only maintains audit and transactional logs of all data sent and received.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

No. At this time, ATLAS does not connect to any systems outside of DHS to facilitate screening and vetting processes. However, while ATLAS may not directly connect to systems external to DHS, it may connect to another DHS system used as an intermediary system to receive data from external partners. For example, ATLAS connects with CBP's Automated Targeting

System (ATS), which may send/receive data to/from external law enforcement and intelligence entities.[55]

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

As ATLAS does not connect or share information directly with systems external to DHS, any external sharing occurs in accordance with the SORNs governing the source systems and is outside the scope of this PIA. In those instances where ATLAS acts as an intermediary system to exchange data with external systems, such sharing is evaluated for compatibility with the source system and the Routine Uses of the applicable SORNs.

6.3 Does the project place limitations on re-dissemination?

Although no information is shared externally from ATLAS, per USCIS policy, USCIS relies on Memorandum of Understanding/Agreements (MOU/A) between USCIS and external organizations to places limitations on re-dissemination of information. External organizations may only share information under the MOU/A when the recipient has an official need, in accordance with the terms of the MOU/A, and allowed by applicable privacy and confidentiality statutes, regulations or policies. Additionally, MOU/As clarify the authority for external organizations and DHS to share immigration and naturalization records and the basic mechanisms established to protect this data.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

ATLAS shares information with interconnected Departmental systems and maintains audit and transactional logs of all data sent and received.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of misuse, unauthorized access to, or disclosure of information.

Mitigation: This risk is mitigated. As ATLAS does not connect to or share information externally, there is minimal risk of improper disclosures related to information sharing. USCIS mitigates this risk by having agreements in place, even for internal use of the data, to ensure uses are consistent with authorized purposes and to place limits on use, sharing, and retention of USCIS data exchanged for screening and vetting. Any future sharing will be memorialized in an

[55] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

information sharing agreement to document appropriate safeguards and place limits on dissemination of information.

Privacy Risk: There is a risk that USCIS may share more information than necessary to facilitate the background checks.

Mitigation: This risk is mitigated. USCIS only shares limited information via ATLAS (e.g., name, date of birth, fingerprint identification number, and A-Number) to facilitate the background checks. This information is necessary to complete the required check. This limited information sharing permits ATLAS to connect to other DHS systems to receive information in return. This information is ultimately used to determine if an individual is eligible to receive an immigration request. Furthermore, USCIS has intra-agency agreements in place for data sharing that restrict its partners from further sharing data beyond the purpose of facilitating background check and screening services. For instance, CBP only utilizes the data for the screening purposes as laid out in an agreement and does not utilize the data elsewise (except for auditing purposes). This agreement prohibits CBP from sharing USCIS data beyond the purpose of supporting background checks and screening.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

ATLAS only maintains audit and transactional logs of all data sent and received. However, an individual may seek access to his or her USCIS records in a source system by filing a Privacy Act or Freedom of Information Act (FOIA) request. Only U.S. citizens and lawful permanent residents may file a Privacy Act request. Account holders 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, he or she may mail the request to the following address:

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

Requests for access to records must be in writing. Such requests may be submitted by mail or in person. If a request for access is made by mail, the envelope and letter must be clearly marked "Privacy Act Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity in accordance with

DHS regulations governing Privacy Act requests (found at 6 CFR Part 5.21), and any other identifying information that may be of assistance in locating the record.

The information requested may, however, be exempt from disclosure under the Privacy Act because FDNS records, with respect to an individual, may sometimes contain law enforcement sensitive information. The release of law enforcement sensitive information could possibly compromise ongoing criminal investigations.

Additional information about Privacy Act and FOIA requests for USCIS records can be found at https://www.uscis.gov/about-us/freedom-information-and-privacy-act-foia.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

ATLAS does not employ any mechanisms that allow individuals to amend erroneous information. ATLAS maintains read-only data, for a short amount of time, obtained from source systems, and USCIS personnel cannot amend ATLAS records directly. ATLAS has a refresh mechanism that updates on a regular basis to reflect any changes in the source systems records; this refresh helps ensure timely and accurate data. While ATLAS does not permit individuals to correct inaccurate or erroneous information itself, U.S. citizens, lawful permanent residents, and other persons with records covered by the JRA are afforded the ability to correct information within source systems and interconnected systems by filing a Privacy Act Amendment request under the Privacy Act. U.S. citizens, lawful permanent residents, and persons covered by the JRA should submit requests to contest or amend information contained in the source system as discussed in Section 7.1. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, the proposed amendment, and any evidence of the correct information. The record must be identified in the same manner as described for making a request for access. If the request is accepted, any amendment would only apply to USCIS-held information. Persons not covered by the Privacy Act are not able to amend their records through FOIA. If non-U.S. persons find inaccurate information in their records received through a FOIA request, they may visit a local USCIS Field Office to identify and amend inaccurate records with evidence supporting their reasons for amendment.

7.3 How does the project notify individuals about the procedures for correcting their information?

ATLAS does not employ mechanisms or procedures to notify individuals on how to amend their information that may be contained within the source system. ATLAS transports data between DHS systems. This PIA and the SORNs and PIAs for source systems explain how individuals may correct erroneous information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that USCIS may not afford an individual adequate opportunity to correct information retrieved by ATLAS from the connected IT systems.

Mitigation: This risk is partially mitigated. ATLAS is not the system of record for any of its stored or transferred data. ATLAS provides a mechanism to access and share data to and from multiple connected systems. The information accessed and retrieved by ATLAS is obtained from connected IT systems. The underlying connected IT systems are fully responsible for any information sent to or provided by ATLAS. It is the responsibility of the connected source system owner to provide procedures for access and redress in accordance with the Privacy Act and FOIA. Individuals may seek more information on access, redress, or correction by reviewing the PIA for the individual system.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

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. The log 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.

ATLAS itself does not have a user interface. ATLAS pushes:

- Results of automated background, identity, and security results to USCIS case and content management systems for USCIS adjudications personnel review; and
- SGNs to FDNS-DS for Gatekeeper manual review.

This process inherits all of the security and access controls established for the interconnected systems that support ATLAS screening. These controls 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.

As a new SGN pattern is conceived, whether it be to detect national security and public safety threats or fraud indicators, criteria are carefully considered by a governance structure. After legal, privacy, policy, and operational requirements are reviewed and approval to move forward has been obtained, technical implementation is crafted and robust testing occurs, prior to deployment. Testing is performed within a testing environment by both technical teams and FDNS personnel prior to deployment to ensure effectiveness of the SGN criteria.

FDNS performs data quality reviews on data streaming through ATLAS for system checks, as well as on SGNs that have fired within FDNS-DS, to ensure compliance with screening requirements, the technical design works as intended, and as approved by the governance structure.

Additionally, FDNS performs data quality reviews on SGNs within FDNS-DS. Every automatically-generated match, or "hit," is reviewed by an officer or an analyst to verify the match is valid and to determine whether the information appears to be actionable. If it does, then the information enters the formal FDNS case management process maintained in FDNS-DS for consideration and possible action by an FDNS Officer. SGNs are routinely and randomly reviewed by the ATLAS Screening and Analysis Team to ensure that the criteria are met and the SGNs are operating as designed.

Routinely, SGN reporting is produced and carefully reviewed which aids in data quality reviews. The reporting is reviewed for authenticity, accuracy, and verity by several levels of FDNS personnel. These provide an accounting for pending triage workloads, work achieved, and adjustments in triaging practices. SGN quality reviews are also performed by the ATLAS Screening and Analytics Team. The team reviews how the SGN fired, if it fired as the system was designed, and analyzes for any improvements that can be made. For certain SGN populations, this is performed on a monthly basis. For others, the checks are performed at random and ad-hoc.

ATLAS is maintained in the Amazon Web Services (AWS), which is a public cloud computing platform designed to meet a wide range of security and privacy requirements (e.g., administrative, operational, and technical controls) that are used by USCIS to protect data in accordance with federal security guidelines. AWS is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host PII.[56] FedRAMP is a U.S. Government

[56] FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. More information available at https://www.fedramp.gov/.

wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services.[57]

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

End users or consumers of information from ATLAS do not access ATLAS directly. Rather, they receive results of automated background, identity, and security checks through their respective adjudicative or investigative case management systems. These users receive the required annual Computer Security Awareness training and Privacy Act Awareness training. In addition, users receive specialized training for their respective case management systems prior to being approved for access to the system. The training addresses the use of the system and appropriate privacy concerns (*e.g.*, SORNs, Privacy Notices). FDNS officers also have several mandatory, job-specific training requirements that include discussions on Privacy Act obligations and other restrictions on disclosure of information.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

USCIS only grants back-end access to ATLAS to authorized personnel (administrator role only) on a strictly need-to-know basis. USCIS audits user access in accordance with the DHS Sensitive Systems Policy,[58] which requires auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

Access to source information is managed in the respective adjudicative case management systems or source systems connected to ATLAS. The end users of ATLAS information are USCIS adjudicative case management systems which have their own access policies. ATLAS communicates with these systems via service-to-service requests and responses. ATLAS does not parse or display any of these messages.

[57] *See* https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.
[58] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

MOAs and MOUs between USCIS and other DHS components, as well as MOAs and MOUs between USCIS or DHS and other agencies, define information sharing procedures for data maintained by FDNS. MOAs and MOUs document the requesting agency or component's legal authority to acquire such information, as well as USCIS' permission to share in its use under the legal authority granted. All MOAs and MOUs must be reviewed by the program and all applicable oversight entities and parties.

Responsible Officials

Donald K. Hawkins
U.S. Citizenship and Immigration Service
Privacy Officer
U.S. Department of Homeland Security
(202) 272-8030

Approval Signature

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

APPENDIX A: ATLAS Connections and Data Sources for Screening

Last updated May 26, 2021

ATLAS connects to the following systems to conduct screening.
USCIS CAMINO[59]
USCIS ELIS[60]
USCIS Global[61]
USCIS TECS by ELIS[62]
USCIS Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR)[63]
CBP TECS Screening Service (TSSV)[64]
CBP Automated Targeting System (ATS) [65]
USCIS Customer Profile Management Service (CPMS)[66]
DHS IDENT[67]
USCIS Fraud Detection and National Security – Data System (FDNS-DS)[68]
USCIS RAILS[69]
DHS Email as a Service (EaaS) Simple Mail Transfer Protocol (SMTP)[70]

[59] *See* DHS/USCIS/PIA-051, CAMINO, *available at www.dhs.gov/privacy*
[60] *See supra* note 13.
[61] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ASYLUM DIVISION, DHS/USCIS/PIA-027(c) (2017), *available* at https://www.dhs.gov/uscis-pias-and-sorns.
[62] *See supra* note 13.
[63] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE CITIZENSHIP AND IMMIGRATION SERVICES CENTRALIZED OPERATIONAL REPOSITORY (eCISCOR), DHS/USCIS/PIA-023(a) (2015), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[64] *See supra* note 12.
[65] *See supra* note 56.
[66] *See supra* note 18.
[67] *See supra* note 19.
[68] See *supra* note 16.
[69] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR RAILS, DHS/USCIS/PIA-075 (2018), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[70] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE EMAIL SECURE GATEWAY, DHS/ALL/PIA-012 (2015 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.