



U.S. DEPARTMENT OF HOMELAND SECURITY OFFICE OF INSPECTOR GENERAL

OIG-26-26

September 23, 2026

FINAL REPORT

Adjudication Errors in Operation Allies Welcome Asylum Files Risked Missing Derogatory Information (REDACTED)



This report contains redacted text that the Department deemed not publicly releasable. Although OIG reviews the Department's redaction requests for an adequate justification to withhold the information, we lack authority to release Departmental information outside the Executive Branch without the Department's consent.

OIG determined that some of the Department's requested redactions lacked adequate justification and we were unable to resolve the matter with the Department. To avoid further delay of the report, we have redacted the contested material pursuant to the Department's request and marked it with an asterisk (*).



DHS OIG HIGHLIGHTS

Adjudication Errors in Operation Allies Welcome Asylum Files Risked Missing Derogatory Information

September 23, 2026

Why We Did This Evaluation

We conducted this evaluation after receiving complaints that the *Ahmed v. DHS* settlement agreement would result in asylum adjudication issues. Based on these complaints, we assessed whether missed aliases or incomplete resolution of potential matches to derogatory records increased in asylum applications from Afghans arriving in the United States under Operation Allies Welcome following the *Ahmed v. DHS* settlement agreement.

What We Recommend

We made five recommendations to improve USCIS' policies, procedures, and guidance related to processing requests for asylum.

OIG Access

During this evaluation, USCIS provided timely responses to our requests for information and did not delay or deny access to information we requested.

What We Found

We found a 40 percent error rate in the adjudication of Operation Allies Welcome (OAW) asylum files we reviewed. The prevalence and type of errors suggest U.S. Citizenship and Immigration Services may have missed opportunities to potentially link names provided by applicants to derogatory information, which in turn would compromise the integrity of alien registration file (A-File) contents that future users rely upon for immigration administration and enforcement activities.

We analyzed a statistical sample of 678 applications from the 13,682 adjudicated applications from the OAW population of Afghan evacuees who resettled in the United States. Within the applications we reviewed, we identified 303 missed aliases, 23 missing security checks, 45 unresolved records, and 115 other documentation issues. **Most errors resulted from missed aliases or incomplete documentation, including two cases related to potential inadmissibility on terrorism-related grounds.** Some errors resulted from an Asylum Officer not identifying a spelling variation of a name or not reprinting and adding a document to the A-file.

We did not observe a statistically significant increase in error rate after the September 2023 DHS settlement agreement that 90 percent of OAW asylum applications would be adjudicated within 150 days (*Ahmed v. DHS* settlement).

USCIS Response

USCIS concurred with all five of our recommendations. We consider all five recommendations open and resolved.



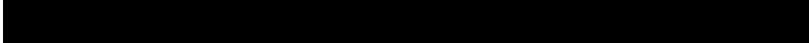
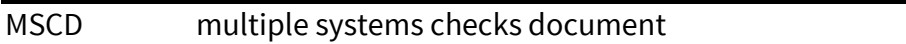
OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Table of Contents

Background	1
Results of Evaluation	5
Key Finding 1: Errors in 40 Percent of OAW A-Files Reviewed	5
Key Finding 2: No Increase in Errors in Adjudicated Applications Post-Settlement Agreement	17
Conclusion	19
Appendix A: Objective, Scope, and Methodology	20
DHS OIG's Access to DHS Information	23
Appendix B: Recommendations, Management Comments, and OIG Analysis	24
Appendix C: USCIS Comments on the Draft Report	28
Appendix D:  ★ Process Diagram	36
Appendix E: Statistical Analysis	37
Appendix F: Report Distribution	40

Abbreviations

AO	asylum officer
ABIS	Department of War Automated Biometric Identification System 
CBP	U.S. Customs and Border Protection
DoW	Department of War
FBI	Federal Bureau of Investigation
FDNS	Fraud Detection and National Security Directorate
IDENT	Automated Biometric Identification System [DHS]  ★ 
MSCD	multiple systems checks document
NCIC	National Crime Information Center
NTC-P	National Targeting Center–Passenger
OAW	Operation Allies Welcome
SAO	supervisory asylum officer
TRIG	Terrorism-Related Inadmissibility Grounds
USCIS	U.S. Citizenship and Immigration Services



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Background

The collapse of the Afghan central government and security forces in 2021 led to a U.S. military operation to evacuate approximately 97,000 individuals from Afghanistan under Operation Allies Refuge and resettle them in the United States under Operation Allies Welcome (OAW).

Any alien who is physically present in the United States, or who arrives in the United States, irrespective of his or her status, may apply for asylum in accordance with statute.¹ An alien may be granted asylum if he or she is not barred from receiving such relief and establishes that:

[he or she is] unable or unwilling to return to, ... [and] avail himself or herself of the protection of, that country [of his or her nationality or last habitual residence] because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion.²

An individual who has been granted asylum will not be removed or returned to his or her country of nationality or last habitual residence.³

To affirmatively apply for asylum, an individual generally files with U.S. Citizenship and Immigration Services (USCIS) Form I-589, Application for Asylum and for Withholding of Removal. Applicants⁴ typically provide supporting documentation, including:

- state or national identification cards;
- employment documentation, affidavits; or
- evidence of country conditions with their Form I-589.⁵

If an alien applies for asylum with USCIS, USCIS will store all submitted information and documentation in the applicant's alien registration file (A-file).⁶

¹ See 8 U.S.C. § 1158(a)(1).

² See 8 U.S.C. §§ 1101(a)(42) and 1158(b)(1)(B)(i).

³ See 8 U.S.C. § 1158(c)(1)(A).

⁴ Although the report refers only to applicants generally, an application will always have a principal applicant and may include derivative applicants. Additional detail is included in our methodology in Appendix A.

⁵ Other types of supporting evidence include newspaper articles, affidavits of witnesses or experts, medical and/or psychological records, doctors' statements, periodicals, journals, books, photographs, official documents, or personal statements or live testimony from witnesses or experts. See <https://www.uscis.gov/sites/default/files/document/forms/i-589instr.pdf>.

⁶ The A-file "contains records involving individuals as they pass through the U.S. immigration and inspection process. The A-File chronicles interactions, including Immigration and Nationality Act enforcement actions, with the U.S. Government." Privacy Impact Assessment for the Person Centric Identify Services (PCIS) Initiative, Dec. 7, 2022, available at <https://www.dhs.gov/sites/default/files/2022-12/privacy-pia-uscis-pia087-pcis-december2022.pdf>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

USCIS oversees lawful immigration to the United States. The Asylum Division within the Refugee, Asylum, and International Operations Directorate adjudicates affirmative asylum applications filed with USCIS. During the Asylum Division's adjudication process, an asylum officer⁷ (AO):

- conducts an in-person interview with the applicant to verify application information and elicit testimony to determine the applicant's eligibility under asylum criteria;
- compares the applicant's name, date of birth, and any aliases⁸ against biographic information in a variety of information systems; and
- reviews and documents evidence indicating that the asylum office biometrically verified the applicant's identity against previously collected biometrics to ensure the person appearing at the interview is the same person for whom biometric security checks were previously submitted.

Biographic Matching

Some screening activities rely on biographic matching between name(s) and date(s) of birth associated with the applicant and records within queried information systems. Our evaluation focused on four biographic screening checks:⁹

- TECS,¹⁰ a law enforcement system operated by U.S. Customs and Border Protection (CBP), "contain[s] temporary and permanent enforcement, inspection and intelligence records relevant to the anti-terrorism and law enforcement mission of [CBP] and numerous other federal agencies that it supports."¹¹
- National Crime Information Center (NCIC), operated by the Federal Bureau of Investigation (FBI), "is an information system that contains records contributed by and accessible to criminal justice agencies nationwide" organized into categories of records, including foreign fugitives, threat screening center, and wanted persons.¹²

⁷ Except for conducting asylum interviews, individuals other than the AO may perform tasks described in this report. However, in this report we attribute all activities to the AO.

⁸ An alias is an additional or assumed name. When collecting aliases, AOs also identify all dates of birth. The definition of what constitutes an alias varies across each biographic system when conducting background, identity, and security checks for affirmative asylum and certain other cases. An alias that requires search in one system may not require a search in another system.

⁹ AOs check other systems, including, but not limited to, Central Index System 2, Person Centric Query Service-Department of Justice-Executive Office for Immigration Review, ENFORCE Alien Removals Module, and Consular Consolidated Database, but we did not review these specific screening checks.

¹⁰ TECS is not an acronym.

¹¹ See 73 FR 77778, 77779 (Dec. 19, 2008). Available at <https://www.govinfo.gov/content/pkg/FR-2008-12-19/html/E8-29807.htm>.

¹² See <https://le.fbi.gov/informational-tools/ncic>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- FBI Name Check “includes a search against the FBI’s Universal Index, which contains personnel, administrative, applicant, and criminal files compiled for law enforcement purposes.”¹³
- Enhanced Fraud Detection and National Security Directorate (FDNS) Review (social media review) is performed by Headquarters FDNS. FDNS “oversee[s] processes for identifying, reviewing, vetting, and adjudicating cases involving national security concerns.”¹⁴ Social media review applies to certain asylum applications,¹⁵ including those submitted by the OAW population, and requires FDNS to screen applicant information against publicly available social media.

Biometric Matching

Other screening activities rely on biometric matching between the applicant’s fingerprint information and fingerprint information in records within queried information systems. Our evaluation focused on three biometric screening checks:

- FBI fingerprint check, which includes a search against “information taken from fingerprint submissions kept by the FBI and related to arrests and, in some instances, [F]ederal employment, naturalization, or military service.”¹⁶
- Automated Biometric Identification System (IDENT), which is “the central DHS-wide system for the storage and processing of biometric data” and “links biometrics with biographic information to establish and verify identities.”¹⁷
- Department of War (DoW)¹⁸ Automated Biometric Identification System (ABIS), which is a “biometrics data repository that processes, matches, and stores biometric identity information data collected [...] during the course of military operations...[including]

¹³ See <https://www.uscis.gov/policy-manual/volume-12-part-b-chapter-2>. FBI Name Check may also be referenced as Criminal Justice Information Services Biographic Verification. On November 25, 2025, the Asylum Division issued new guidance on the FBI Name Check process. Per the guidance, effective December 09, 2025, National Vetting Center (NVC) checks satisfy FBI Name Check requirements.

¹⁴ See <https://www.uscis.gov/about-us/organization/directorates-and-program-offices/fraud-detection-and-national-security-directorate>.

¹⁵ See [REDACTED]

¹⁶ See <https://www.justice.gov/tribal/page/file/1354861/dl>.

¹⁷ See <https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf>. As described in our methodology in Appendix A, we performed limited analysis on IDENT.

¹⁸ Pursuant to Executive Order 14347, “Restoring the United States Department of War,” September 5, 2025, the Department of Defense uses the secondary title Department of War where the use of such title “does not create confusion with respect to legal, statutory, or international obligations.” See also Memorandum from the Secretary of War, “Department of War Secondary Titles” (Oct. 10, 2025).



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

warfighting, intelligence [...] force protection, base access...[and] counterterrorism [...].” ABIS also includes biographic information collected by [DoW].¹⁹

Screening Process

The AO uses Global, the Asylum Division’s case management system, to identify and review certain biographic and biometric security check information.²⁰ Global indicates whether a security check resulted in no match or a potential match (indicated as “no hit” or “hit” for some checks) to a record, which includes information that may warrant further investigation or clarification. If the information matches and is derogatory (i.e., national security concerns, criminal convictions, and other misconduct), it may ultimately lead to an unfavorable asylum decision by USCIS.

The AO must review all potential matches to determine whether there is an actual match between the applicant and the subject of the record. If the AO determines there is a match, he or she must take certain steps to resolve that match. Generally, the AO must assess the effect of the content of the record on the applicant’s eligibility for asylum. For example, the *Immigration and Nationality Act*²¹ bars individuals associated with certain activities from obtaining asylum.²²

The AO must then document his or her resolution of the match and results of all background and security checks on a document named the [REDACTED], which this report refers to as the multiple systems checks document (MSCD).²³ [REDACTED]

★

24

¹⁹ See 89 FR 92665, 92665 (Nov. 22, 2024). Available at <https://www.govinfo.gov/content/pkg/FR-2024-11-22/html/2024-27403.htm>.

²⁰ FDNS initiates social media checks for the Asylum Division later in the application process.

²¹ See 8 U.S.C. § 1101 et seq.

²² These activities include, but are not limited to, participating in the persecution of another on account of a protected ground (race, religion, nationality, membership in a particular social group, or political opinion), conviction of a “particularly serious crime,” and engaging in “terrorist activity.” See 8 U.S.C § 1158(b)(2)(A).

²³ MSCD is an OIG created term.

²⁴ Redactions in this report marked with an asterisk were requested by the Department without adequate justification. OIG has redacted the contested material because OIG lacks authority to release Departmental information outside the Executive Branch without the Department’s consent.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Expedited Asylum Processing Requirements for the OAW Population

The *Afghanistan Supplemental Appropriations Act, 2022*²⁵ (the Act) requires expedited processing for the OAW population's asylum applications. The Act requires USCIS to interview an OAW asylum applicant within 45 days of the filing of the application, without exception.²⁶ This differs from the requirement for non-OAW asylum applicants, which allows 45 days for the interview, but permits additional time for exceptional circumstances.²⁷ The Act also requires USCIS to adjudicate OAW asylum applications within 150 days of the filing of the application, absent exceptional circumstances,²⁸ while the timeframe for the non-OAW applications is 180 days, absent exceptional circumstances.²⁹

In April 2023, a group of plaintiffs sued DHS (*Ahmed v. DHS*),³⁰ alleging the Department was not adjudicating asylum applications from the OAW population in timeframes consistent with the Act. On September 6, 2023, DHS and the plaintiffs settled the lawsuit. DHS agreed to adjudicate asylum applications from the OAW population according to a schedule in which USCIS ultimately would adjudicate 90 percent of asylum applications from the OAW population within 150 days.³¹

We received complaints from USCIS employees expressing concerns about the effect of the *Ahmed v. DHS* settlement agreement (settlement agreement) on the asylum adjudication process due to the shortened timeframe for adjudication. More specifically, complainants worried settlement timelines would negatively impact proper supervisory review of cases. We conducted this evaluation to determine whether missed aliases or incomplete resolution of potential matches to derogatory records increased following the settlement agreement.

Results of Evaluation

Key Finding 1: Errors in 40 Percent of OAW A-Files Reviewed

We identified errors in 40 percent (269) of the files we reviewed,³² regardless of whether the adjudication occurred before or after the settlement agreement. To determine this, we first identified 13,682 adjudicated applications from the OAW population meeting our criteria. From

²⁵ See Pub. L. No. 117-43.

²⁶ *Id.* at Section 2502(c)(1).

²⁷ See 8 U.S.C. § 1158(d)(5)(A)(ii).

²⁸ Pub. L. No. 117-43, Section 2502(c)(2).

²⁹ See 8 U.S.C. § 1158(d)(5)(A)(iii).

³⁰ *Ahmed v. DHS*, 4:23-cv-01892 (N.D. Ca. 2023).

³¹ See *Ahmed v. DHS*, 4:23-cv-01892-JST (N.D. Ca. Sept. 11, 2023). Available at <https://www.uscis.gov/sites/default/files/document/legal-docs/DKT103-2SettlementAgreement.pdf>.

³² As described in our methodology, USCIS reviewed most but not all error types and, particularly for resolution errors, did not always agree with our categorization of errors.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

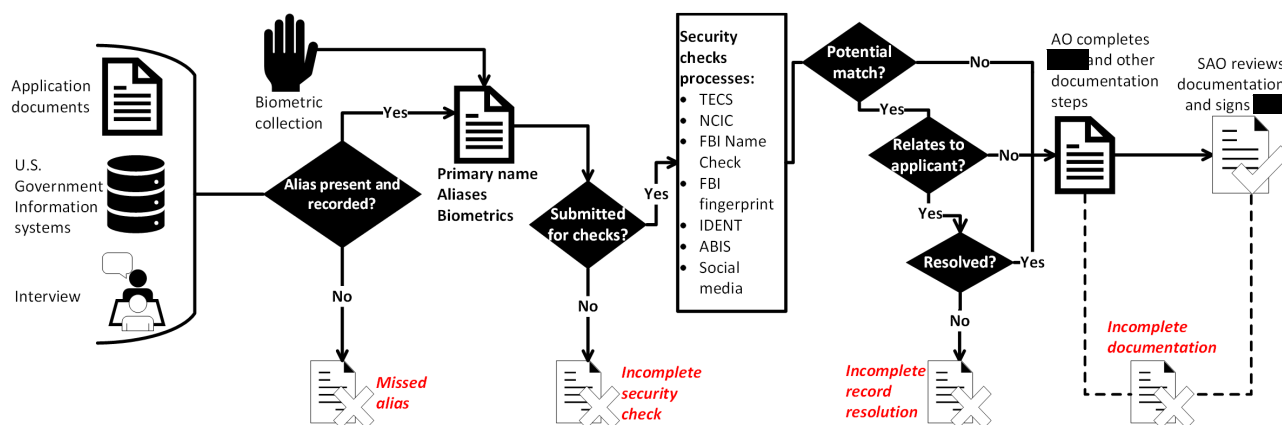
this, we reviewed a statistically valid random sample of 678 applications, including applications adjudicated before and after the settlement agreement.³³

For each of the 678 applications, we reviewed all documents available to the AO at the time of adjudication related to four general categories: (1) aliases, (2) security checks, (3) resolution of potentially derogatory records, and (4) overall documentation. We reviewed the 678 files in our sample related to these four categories to determine whether the AOs:

- identified all aliases;
- completed all security checks;
- resolved all potential matches to derogatory records; and
- completed all required documentation steps.

If the AO missed any of the four, we considered that to be an error. For each of these categories we counted errors and files with at least one error in that category. We also looked at total errors from all categories combined and the total number of files with at least one error. Figure 1 depicts our file review process and Table 1 summarizes the types of errors we identified.

Figure 1. Adjudication Process Relevant to Our Evaluation



Source: DHS Office of Inspector General analysis based on USCIS information

³³ The 678 applications were the basis for a statistical analysis discussed in the second finding.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Table 1. Summary of Errors Identified During Application Review

Error type	Total errors	Files with errors	Percent of files with errors
Missed Aliases	303	169	25
Incomplete Security Check	23	23	3
Incomplete Record Resolution	45	45	7
Incomplete Documentation	115	96	14

Source: OIG analysis

Most errors we identified resulted from missed aliases or incomplete documentation. Although the cause and effect of any error is fact-specific, these types of errors may result from omissions, such as an AO not identifying a spelling variation of a name or not reprinting and adding a document to the A-file. We did not assess the actual effect of any error we identified, including whether an error would have impacted an applicant's asylum eligibility. However, the overall prevalence of errors suggests USCIS may have missed opportunities to link names provided by applicants to potentially derogatory information, if any existed, that corresponded to that name, compromising the integrity of A-File contents upon which future users rely for immigration administration and enforcement activities.

Missed Aliases in 25 Percent of Files

We identified aliases that the AO did not enter into Global — the Asylum Division's case management system — in 169 files (25 percent). **We found some files with multiple missed aliases, resulting in a total of 303 missed aliases in our sample, precluding potential matches between that alias and records in subsequent security system checks.** Table 2 shows the distribution of missed aliases, including one file with 12 missed aliases.

Table 2. Missed Alias Distribution

Number of missed aliases	Number of files	Total number of missed aliases
1	107	107
2	32	64
3	15	45
4	6	24
5	2	10
6	2	12



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

7	3	21
8	1	8
12	1	12
TOTAL	169	303

Source: OIG analysis

USCIS background and security check procedures require AOs to review application documentation for aliases, *

*
The AO enters all aliases he or she identifies into Global to facilitate these checks.

In 2022, the Asylum Division created an *³⁴ that provides guidance on *

*
35

*
*

During * the AO examines an applicant's entire application file, which for some is voluminous and includes numerous aliases. For example, we found one file in our sample with 124 aliases.³⁶ Moreover, AOs must perform the activity while maintaining adjudication timelines. Based on these factors, we found that AOs may be unable to entirely avoid missed aliases.

³⁴ *
³⁵ *

³⁶ The median was two aliases per file in our sample.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Incomplete Security Checks in 3 Percent of Files

We identified 23 files (3 percent) with missing security checks results, all of which related to either FBI Name Check or TECS, potentially missing matches between the applicant and a derogatory record in one of the systems.³⁷ We found this type of error once in each of the files, for a total of 23 errors.

Global facilitates biometric and biographic checks of the applicant's primary name, aliases, and biometrics during the screening process. For biometric searches, USCIS sends applicants' biometric information to FBI and DHS' Office of Biometric Identity Management, which performs searches. For biographic matching, Global facilitates searches within each system — according to that system's search rules. We looked at three biographic security checks initiated through Global — TECS, NCIC, and FBI Name Check. [REDACTED]

Missed FBI Name Check searches accounted for 57 percent (13 of 23) of the missing security checks we identified. AOs must manually initiate the FBI Name Check search for certain aliases within Global, or for expired results. This contrasts with TECS, where Global automatically initiates security checks and uses business rules to prevent an AO from completing adjudication by granting asylum if checks are incomplete.³⁸ [REDACTED] *

39

40

Ten of 23 (43 percent) of the missing security checks that occurred were related to TECS. Nine of these errors were in applications USCIS administratively closed.⁴¹ When USCIS administratively closes an application, in certain cases the AO must still complete the TECS security checks on the

³⁷ Global displays TECS and NCIC security check results together. When we identified a missing TECS security check, we did not also separately record a missing NCIC security check.

³⁸ [REDACTED]

³⁹ [REDACTED]

⁴⁰ As described in our methodology in Appendix A, we were conservative in assessing [REDACTED]

⁴¹ USCIS may administratively close some asylum applications for various reasons, including when an applicant initiates an administrative closure by withdrawing his or her application; or the component identifies a conflict of jurisdictional authority (e.g., applicant is in removal proceedings); or the component determines the applicant has abandoned his or her asylum application. AOs must complete security checks only for certain types of administratively closed cases.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

primary name⁴² and document results of these checks on the MSCD. Although administratively closed applications were only 3 percent of the files we reviewed, they accounted for 39 percent (9 of 23) of the files we identified with security check errors.

The remaining missing TECS security check resulted from a technical issue. In this instance, the

★
As a result, although the AO identified the name and manually added it to Global, Global did not search the name in TECS. During our fieldwork, USCIS identified the technical issue that caused the error and later told us it submitted a request to address the issue.

Incomplete Resolution of Potentially Derogatory Records in 7 Percent of Files

We identified 45 files (7 percent) with incomplete resolution of potential matches to derogatory records, risking improper adjudication of the application, which may have an additional impact during adjudication of a future immigration benefit application. We found this type of error once in each of the files, for a total of 45 errors.

When an AO submits applicant information for security checks, the process may identify a potential match between that information and a derogatory record. For potential biographic matches, the AO must first determine whether there is an actual match between the applicant and the subject of the record. ★

★ If the AO determines there is an actual match between the applicant and the security checks record, he or she must assess whether the information in the record is derogatory, affecting the applicant's eligibility for asylum. ★

★ The errors we identified were related to resolution of potentially derogatory records found in ABIS, FBI fingerprint checks, NCIC, and TECS, as described below.

ABIS

Fifty-one percent (23 of 45) of resolution errors related to ABIS, which is a biometric system that does not require the AO to assess whether the hit ★. Instead, CBP reviews records that match the applicant and determines if there is derogatory information related to the applicant. In addition to considering the CBP determination, the AO must review all ABIS records

⁴² TECS checks help USCIS, ★

★



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

associated with the applicant and determine the impact of the information on asylum eligibility.

[REDACTED] All 23 ABIS errors we identified occurred because an AO did not include ABIS details in the A-file. Within our sample, many ABIS records were non-derogatory. [REDACTED]

FBI Fingerprint Check

We identified four errors related to resolving matches between applicants and FBI fingerprint check records.⁴³ FBI fingerprint matches generally relate to records of arrests documented in an Identity History Summary.⁴⁴ When there is a match, the AO must obtain, print, and include the Identity History Summary in the A-file. In two of the four FBI fingerprint resolution errors we identified, the AO did not include the Identity History Summary document in the A-file. However, unlike ABIS, the AO must assess the substance of a match to an FBI fingerprint record. Without the Identity History Summary, we could not assess the resolution substantively.

The remaining two FBI fingerprint check errors related to our review of Asylum Division guidance.

[REDACTED] 45 *

NCIC

We found 13 errors related to resolving potential matches to NCIC records. Because a hit indicates only a potential match, the AO must determine whether the NCIC record is associated with the applicant. To do so, the AO compares applicant information to information in the NCIC record.

[REDACTED] All the errors we identified related to completion of the form required for potential matches [REDACTED]

⁴³ FBI fingerprint checks results in a biometric match that does not require the AO to assess whether the hit [REDACTED] *

⁴⁴ The Identity History Summary includes information on the record that matched to the applicant.

⁴⁵ *



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

TECS

We found five errors related to resolving potential matches to TECS records. [REDACTED]

[REDACTED] *

Based on files in our sample, applicants occasionally matched with TECS records that were not based on specific derogatory information associated with the applicant. For example, some of the matches in our sample [REDACTED], which would not affect the applicant's ability to apply for asylum. However, because these records still related to the applicant, the AO had to complete a [REDACTED] *, and we identified two errors relating to this requirement. In one instance, an SAO did not sign the [REDACTED] * and in the other instance, the AO did not address all related TECS records in the [REDACTED] *.

The other three TECS resolution errors related to specific applicant records. In the first resolution error, the AO did not identify the reason for the resolution of Department of State information.⁴⁶ [REDACTED] *

[REDACTED] | [REDACTED] .⁴⁷

The A-file included a [REDACTED] * stating only that the AO asked FDNS to determine whether the TECS hit [REDACTED] * but did not actually resolve the record itself. Because the MSCD was marked as having a related TECS record, policy required resolution of that record.⁴⁸

The steps to resolve potential matches can be lengthy and depend on the security check the AO is performing. For one file within our sample, the TECS/NCIC security checks for an applicant with a common name returned more than 1,500 potential match results. The AO must review each result to determine whether there is an actual match between the applicant and the subject of the record, and then resolve any matches as required.

Overall, some of the resolution errors we found may have resulted from omissions, such as AOs not including paperwork. These types of errors might hinder the ability for a future user of an A-file to understand the adjudication. For example, a future user would see an ABIS hit recorded in the A-file but not see the ABIS information itself. Other instances of incomplete resolution were more substantive in nature, such as an AO not establishing whether the applicant was the

⁴⁶

⁴⁷

⁴⁸

[REDACTED] *

[REDACTED]

[REDACTED] *

[REDACTED] | [REDACTED]



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

subject of a national security record. These errors might affect a future user's understanding of an applicant's immigration benefit eligibility. For example, an unresolved potential match to an arrest record or national security record might raise questions about an applicant's eligibility for asylum or a future immigration benefit.

Documentation Errors in 14 Percent of Files

Within our sample of 678 files, we identified 96 files (14 percent) with documentation errors, such as missing required paperwork or incomplete MSCDs. Some files had multiple issues, resulting in a total of 115 documentation errors.

The AO must complete certain documentation steps related to the security checks process. AOs must record the results of each security check on a MSCD.⁴⁹ The MSCD lists each security check in a field and includes [REDACTED]

[REDACTED]

[REDACTED]

MSCD

The largest source of documentation errors were found on the MSCD, accounting for 75 percent (86 of 115 errors) of the documentation errors we identified. Of these 86 errors relating to MSCD completion, we identified:

- 49 errors involved an issue with an MSCD [REDACTED], where the AO incorrectly [REDACTED];
- 26 errors resulted from the SAO [REDACTED] the MSCD; and

⁴⁹ As described in our methodology in Appendix A, we addressed missing documentation related to a specific security checks system in the resolution section. In this section, we address missing documentation that is not specific to a single security checks system.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- 11 errors resulted from the MSCD [REDACTED].

Within our sample, we identified some files that used an electronic MSCD. The electronic MSCD merges Global's security checks tab into the MSCD, potentially preventing errors related to incomplete or incorrect information. We found that improper completion of MSCDs accounted for 18 percent of the total errors we identified in our sample. Adoption by USCIS Asylum Division of the electronic MSCD might offer opportunities for additional controls to reduce MSCD errors and ensure compliant documentation.⁵⁰

Missing Paperwork

We found required paperwork missing from the A-file, such as copies of completed security checks, accounting for 25 percent (29 of 115) of documentation errors, the consequences of which range from an administrative inconvenience to missing information directly related to inadmissibility.

After final adjudication, the AO must add the completed MSCD to the A-file. Like the MSCD, Global's security checks tab contains details of each security check. AOs must include a copy of the completed security checks tab in the A-file. Within our sample, instances of missing copies of completed security checks results generally occurred when the AO performed more than one type of security check multiple times but did not include a copy of the most recent completed security check results in the A-file. We also identified two files that were missing the assessment⁵¹ or the interview notes, which are required asylum documents.

⁵⁰ As an example of potentially similar control, a USCIS official told us Global would not allow a case to proceed with expired TECS checks, and we did not identify any expired TECS checks within our sample.

⁵¹ The assessment documents the reasoning of the AO's decision and the facts upon which it is based.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Documentation Resolving Possible Terrorism-Related Inadmissibility Grounds (TRIG)

We identified errors of missing paperwork⁵² related to documentation required when an AO identifies evidence that an applicant may be subject to TRIG.⁵³ If the AO believes a TRIG exemption may be warranted, the AO must complete the TRIG exemption worksheet to recommend either granting or denying the exemption. At least two levels of appropriate authorities above the AO must approve this document. One of the errors resulted from the AO including TRIG analysis in the assessment, but the file did not include a TRIG worksheet. This means a second level authority, such as a section chief, did not approve the analysis, as required. The other error resulted from a completed TRIG worksheet that both the SAO and section chief signed, but neither marked a box indicating whether they approved or disapproved the AO's analysis.

The potential consequences of documentation errors vary according to the document. Missing printouts of the security checks page or MSCD [REDACTED] might be inconsequential beyond inconvenience because the information is generally available in another location. However, other missing documents have a greater impact. A missing assessment or interview notes might mean that USCIS has no record of why it believed the applicant warranted asylum and limited information or analysis of whether mandatory bars⁵⁴ apply.⁵⁵ Similarly consequential are errors related to the SAO signature and the inadmissibility bar process, which mean USCIS did not follow the process it created to ensure an applicant's security checks, and any national security concerns relating to that applicant, are reviewed and approved at an appropriate level. Ultimately, documentation errors or missing documentation at the beginning of the adjudication process could compromise the integrity of A-File contents, which users rely upon during future immigration administration and enforcement activities.

Ambiguous Guidance Regarding Social Media Review

We found at least eight potential resolution errors related to social media review but did not count them because of ambiguity in the guidance. During social media review, FDNS performs the initial action and returns a Record of Action to the AO describing the results of its work. In

⁵² These two errors are part of the 29 errors we identified as missing paperwork introduced in the previous section.

⁵³ Individuals who are members of terrorist groups or otherwise have engaged in terrorism-related activity are generally ineligible for immigration benefits, including asylum. The Secretaries of State and Homeland Security may grant exemptions based on the nature of the applicant's activity. As an example, an exemption may be available if an applicant acted under duress. See <https://www.uscis.gov/laws-and-policy/other-resources/terrorism-related-inadmissibility-grounds-trig>.

⁵⁴ An applicant may be barred from a grant of asylum for certain actions, including participating in certain types of persecution or posing a danger to the U.S. See <https://www.uscis.gov/humanitarian/refugees-and-asylum/asylum/asylum-bars>.

⁵⁵ Although we did not find these documents during our file review, it is possible a copy exists in some other format.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

the eight files where we identified an issue, FDNS questioned an applicant's social media content, generally noting the content as "of interest" or "derogatory." The social media content within our sample included:

[REDACTED]

We did not identify a section of the assessment or a memo where the AO addressed the impact of this content on the applicant's asylum eligibility. MSCD guidance states:

[REDACTED]

We identified these files as potential resolution errors based on our interpretation of this language. When we asked about this issue,⁵⁶ a USCIS official said FDNS' marking of the documents is preliminary and the AO determines whether the information is "of interest" or "derogatory." We reviewed the [REDACTED] ★ [REDACTED] for additional guidance, [REDACTED]

[REDACTED] Based on this ambiguity, we chose not to count these eight potential errors in our analysis of the files.

Regardless of whether USCIS policy requires the AO to address information FDNS has labeled as derogatory or of interest, based on files within our sample, the AO generally did not address this information. This practice resulted in unexplained information in the A-file that was labeled as derogatory or of interest. [REDACTED]

[REDACTED]

⁵⁶ As described in our methodology in Appendix A, USCIS reviewed errors we identified except some documentation errors. For the errors USCIS did not confirm, we only counted the error if the criteria supporting the error was sufficiently clear.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Recommendation 1: We recommend the Asylum Division Chief determine whether it is feasible to establish, and regularly assess compliance with, a benchmark for expected error rate during the security checks process. This analysis should identify if any specific type of error is incompatible with the integrity of the security checks process.

Recommendation 2: We recommend the Asylum Division Chief evaluate methods and implement changes to the [REDACTED] ★ [REDACTED] policy and process to increase the effective identification and recordation of aliases to ensure they are processed for security checks.

Recommendation 3: We recommend the Asylum Division Chief identify and implement additional information system controls or other changes to ensure all required security checks are performed before an application is administratively closed.

Recommendation 4: We recommend the Asylum Division Chief assess whether transitioning all adjudications to an electronic [REDACTED] would improve [REDACTED] completion consistency.

Recommendation 5: We recommend the Asylum Division Chief identify and implement changes to ensure the Alien-file documents the asylum officer's consideration of information identified in FDNS' Record of Action regarding social media reviews.

Key Finding 2: No Increase in Errors in Adjudicated Applications Post-Settlement Agreement

We found that missed aliases and incomplete resolution of potential matches to derogatory records did not increase following the settlement agreement. As part of this work, we additionally noted that there was no increase in missed security checks or documentation errors after the settlement agreement.

We performed this analysis for asylum applications before and after the settlement agreement to determine whether error rates were higher after the settlement agreement, as suggested by complaints.

As depicted in Figures 2 and 3, error rates within our sample were higher after the settlement agreement in some categories but were not statistically significant after applying statistical analysis to infer the results of the 678 files that we reviewed to all 13,682 applications meeting



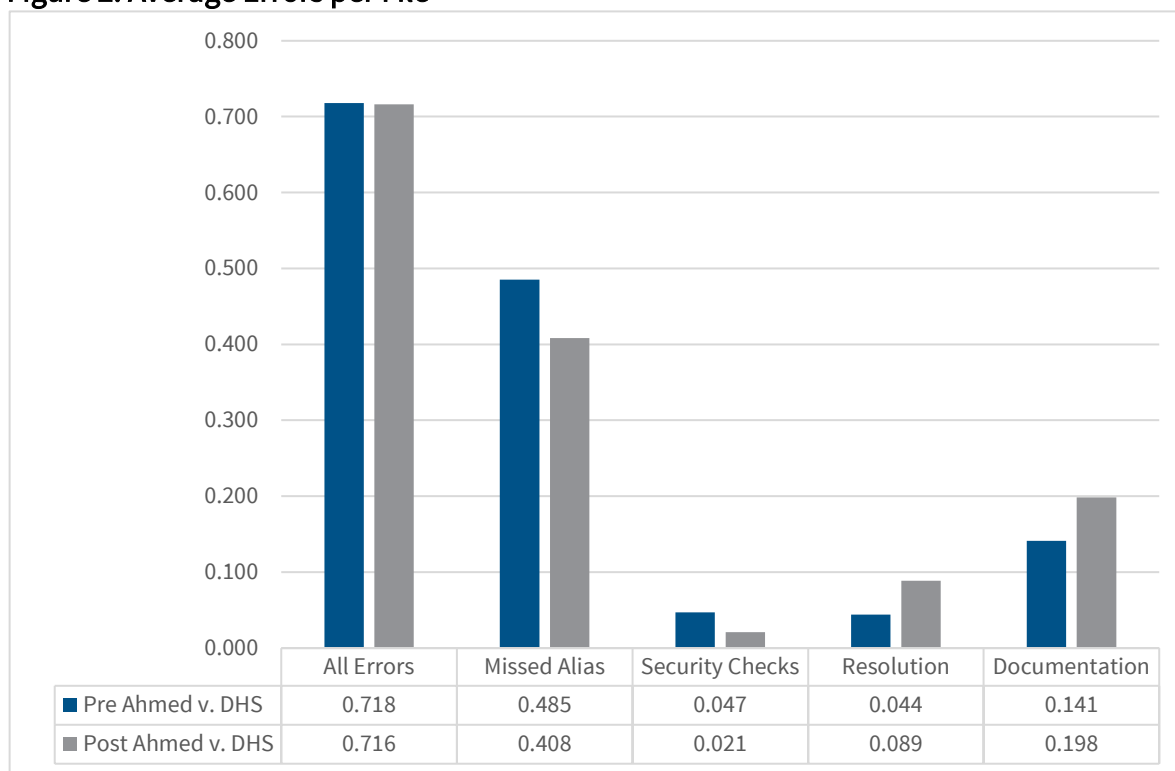
OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

our criteria.⁵⁷ We therefore determined that the settlement agreement did not result in higher error rates. Appendix E provides additional detail on our statistical analysis.

On average, we identified 0.716 errors per file after the settlement agreement, which was slightly lower than the 0.718 errors per file we identified before the settlement agreement. The average error rate post-settlement agreement was higher for resolution and documentation errors. However, the differences in errors rates were not statistically significant and do not indicate an increase in errors after the settlement agreement. Figure 2 depicts average errors per file for each of the four categories we checked as well as all errors.

Figure 2. Average Errors per File



Source: OIG analysis

Overall, the percentage of files with errors post-settlement agreement was smaller than the percentage pre-settlement agreement, although a higher percentage of post-settlement agreement files had resolution and documentation errors. Neither of these two instances with higher percentages of files with errors were statistically significant and therefore do not indicate

⁵⁷ Statistical significance means that in accordance with a defined confidence level – 95 percent in our analysis – the difference in error rates in our sample did not result by chance.

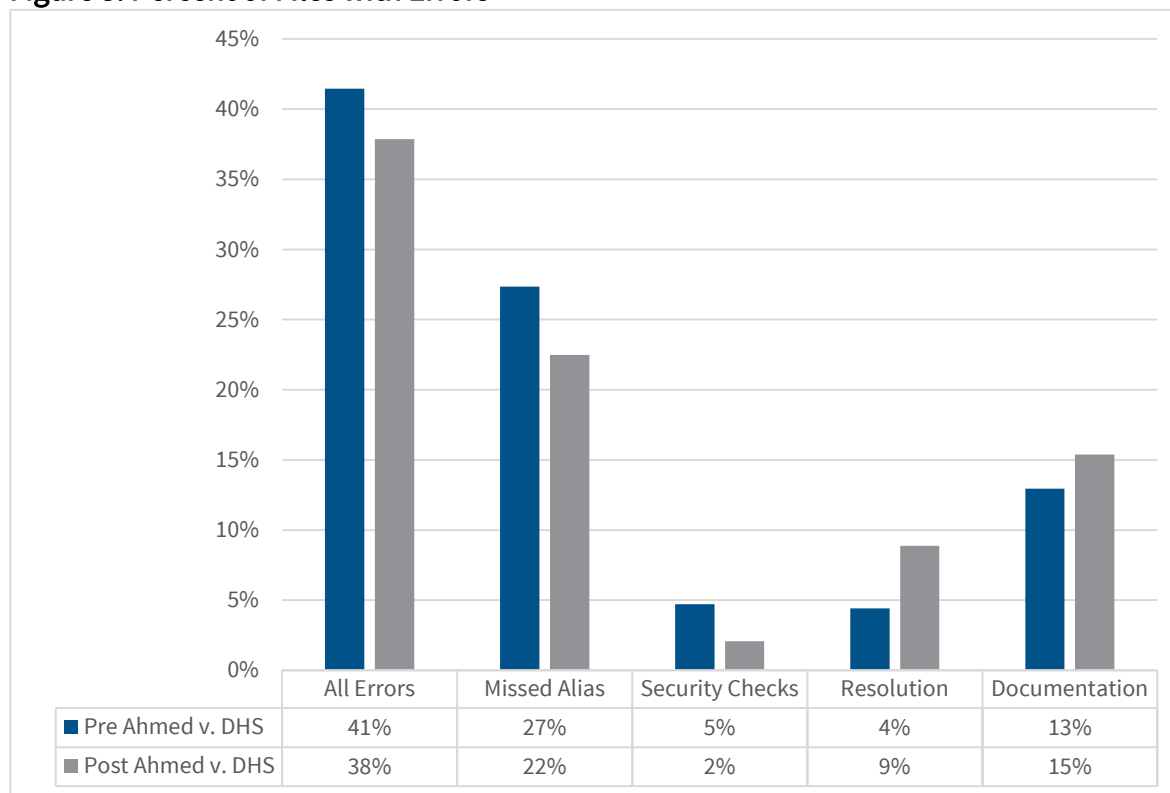


OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

an increase in errors after the settlement agreement. Figure 3 depicts the percentage of files that had at least one error.⁵⁸

Figure 3. Percent of Files with Errors



Source: OIG analysis

Conclusion

We identified errors in 40 percent of the applications within our sample, but did not find that the settlement agreement impacted error rates for asylum applications submitted by individuals paroled into the United States under OAW. Although many of the errors we identified may have resulted from minor omissions, they still resulted in USCIS missing opportunities to identify potential matches between names the applicant provided to USCIS and derogatory information. Some of the errors we identified in the adjudication process could negatively impact the integrity of the A-files, which USCIS relies on for future immigration administration and enforcement activities.

⁵⁸ Because a file may have had errors in more than one error category, the percentage for all errors may be smaller than the sum of individual error categories.



Appendix A: Objective, Scope, and Methodology

Our objective was to determine whether missed aliases or incomplete resolution of potential matches to derogatory records increased following the *Ahmed v. DHS* settlement agreement.

Our evaluation publication was significantly delayed by three Government shutdowns in FY 2026, which covered 56 percent of the fiscal year through May 1.

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107-296) by amendment to the *Inspector General Act of 1978*.

We conducted fieldwork for this evaluation from March 2024 to January 2025. Our scope was asylum applications submitted by individuals paroled into the United States as part of OAW. We limited our review to applications with final adjudication completed before February 6, 2024, which was the date an additional security check was instituted and thus would not be represented in applications completed both before and after the settlement agreement. Our fieldwork included:

- reviewing policies, procedures, and guidance related to processing, adjudicating, and tracking OAW asylum applications;
- interviewing USCIS employees involved in various program operations related to OAW asylum application processing; and
- analyzing data USCIS provided from both information systems and its own data collection methodology.

Additionally, during fieldwork, we reviewed a sample of OAW asylum applications satisfying the following criteria:

- final adjudication complete;
- principal applicants;⁵⁹ and
- applicant age between 14 and 79 (inclusive).⁶⁰

⁵⁹ The principal applicant is the person who signs the asylum application, with USCIS assessing the merits of his or her claim. A principal applicant may include in his or her application a spouse and unmarried children under the age of 21 years; otherwise known as derivative applicants. See <https://www.uscis.gov/sites/default/files/document/forms/i-589instr.pdf>.

⁶⁰ We excluded applicants under 14 years old or over 79 as those age groups have different vetting requirements outside the scope of our review.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

We selected a minimum number of applications from before and after the settlement agreement. Applications reviewed before settlement included those completed and served by September 6, 2023. Applications reviewed after settlement included those completed and served on or after September 7, 2023, and by February 6, 2024. We worked with OIG's Data Services Division to randomly select 500 applications from both before and after the settlement agreement. Depending on how an applicant applied, USCIS maintains documents in physical or electronic format. Our sample included both formats. We requested files for applications from these pools according to their number in the pool, which was randomly assigned. To minimize impacts to ongoing operations, we designed our sample to be larger than the number of files we needed to review so we could skip applications if the A-file was in use at the time we requested it.

To meet our statistical analysis goal, we reviewed 678 files. For applications with physical documentation, we reviewed paper A-files during site visits to USCIS' Asylum Division field office in Arlington, VA, and to USCIS' National Benefits Center in Lee's Summit, MO.⁶¹ For electronic applications, we reviewed copies of documentation USCIS provided to us electronically.⁶² We reviewed files consistent with USCIS' demonstration of a supervisory review, regardless of file type.⁶³ Our review did not include reassessing AO's decisions. For example, we reviewed whether the AO determined whether an applicant matched to a potentially derogatory record, but did not review the AO's decision itself. We also reviewed files consistent with a methodology process we derived from applicable USCIS criteria, including:

- FDNS' [REDACTED] ★ [REDACTED];
- Affirmative Asylum Procedures Manual;
- ★ [REDACTED]; and
- [REDACTED]

Before application review, we shared a detailed methodology with the Asylum Division. We also shared the methodology with a section chief who was initially assigned as a point of contact. We adjusted our methodology as appropriate. Most notably, our initial methodology relied on the MSCD but did not account for errors on the MSCD. As we identified these errors during application review, we adjusted our methodology to record them.

⁶¹ Only one person can possess a physical A-file at a time. If an applicant in our sample had subsequently applied for an additional benefit, his or her A-file might be in use at the time we requested it. Many A-files in our sample were in use, especially by USCIS' National Benefits Center. We were able to review these A-files at the National Benefits Center, which minimized disruption to benefit processing while allowing us to perform fieldwork without enlarging our sample pool.

⁶² For electronic A-files, the Asylum Division electronically transferred copies of documents attached to the asylum application in Global. Under this process, the availability of relevant documentation was not impacted.

⁶³ At the outset of application review, a section chief who was assigned as a point of contact demonstrated how supervisory review was performed.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

For missed alias identification, an OIG primary reviewer checked all documents available to an AO at the time of asylum adjudication to identify aliases. The reviewer generally recorded all aliases on a separate document, then compared aliases we identified to the TECS search combinations on the security checks printout. If the reviewer identified an alias that was not searched in TECS, a second OIG employee reviewed both the source document to confirm the alias and the TECS searches to confirm the AO had not run the alias. If the second OIG reviewer agreed the AO missed the alias, the primary reviewer took pictures of the error and sent the error documentation to a USCIS point of contact for confirmation. Originally, we recorded only the alias source but later added the TECS search page to better document the error.

For missed security checks, the primary reviewer reviewed the MSCD and the security checks printout. The reviewer assessed whether these documents indicated the AO performed required checks for TECS, NCIC, FBI Name Check, IDENT, FBI fingerprint, ABIS, and social media review. Although our security checks process included checking whether aliases were run, we did not also consider a missed alias as a missed security check. For TECS and NCIC, we checked whether there were results for each alias. For FBI Name Check, we identified a missing security check error [REDACTED]. Our checks for IDENT were limited to assessing whether the MSCD marking corresponded to the security checks tab. Upon submission of potential security checks errors to USCIS, USCIS occasionally provided an updated copy of the security checks printout that demonstrated the security check had been completed. In these cases, we would move this error type to missing documentation.

For missed error resolution, we assessed whether the AO completed all steps outlined in various USCIS criteria to resolve matches or potential matches within each security check system. For some systems, our concept of missed resolution differed from USCIS' definition. Generally, we looked for technical resolution, i.e., according to criteria, whereas USCIS referenced substantive resolution. Resolution of ABIS matches was a common source of this divergence. USCIS noted that the National Targeting Center–Passenger substantively resolved these matches, with the AO simply recording the results of the National Targeting Center–Passenger's resolution. However, we considered the technical issue of the AO not including copies of the matches in the A-file as a resolution error. We used the same error review process described for missed aliases and photographed resolution errors. However, like security checks errors, the evidence of some resolution errors was the absence of documentation, which we could not photograph without copying the entire file.

For documentation issues, if the documentation applied to resolving an error in a specific security check system we considered it as a resolution error, and if not, a distinct, missed documentation error. Because we did not identify them as errors on the form we created to record our file review results, documentation errors generally were identified only by a primary



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

reviewer without secondary review within OIG or review by USCIS. As we identified the relative frequency of documentation issues, we photographed them.

We recorded the results of application review on a search form specific to each applicant. Upon completion of application review, we performed data cleaning and standardization activities of search form data to enable analysis and reporting. We performed additional analysis of criteria on all errors USCIS did not confirm, followed up with USCIS when necessary, and adjusted a small number of errors based on additional discussions and analysis. Most notably, we decided not to count certain missed aliases as errors based on our determination that the missed aliases were based on the AO's judgment. We did not count these as errors because USCIS policy allowed AOs not to add the names to Global. The total number of instances of AO judgment that we did not count would have added 26 files with errors and 51 total errors to the missed alias category. Except for certain errors, [REDACTED] ★ [REDACTED] that is described in the report, we are not aware what actions, if any, USCIS took in response to errors it confirmed.

We conducted this evaluation under the authority of the *Inspector General Act of 1978*, 5 U.S.C. §§ 401–424, and according to the *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency.

DHS OIG's Access to DHS Information

During this evaluation, USCIS provided timely responses to our requests for information and did not delay or deny access to information we requested.



Appendix B:

Recommendations, Management Comments, and OIG Analysis

USCIS provided management comments on a draft of this report. We included the comments in their entirety in Appendix C. We also received technical comments from USCIS on the draft report; we revised the report as appropriate. We also considered USCIS' requests for the redaction of sensitive information contained in the report. We granted the requests by redacting or rewording report language to remove sensitive language. Redactions for requests that were submitted without adequate justification are marked with an asterisk. USCIS concurred with all five recommendations, which we consider open and resolved. A summary of the USCIS response and our analysis follows.

In its comments, USCIS stated that security check requirements for administrative closures changed in January 2024, and it was unable to verify the report's count of errors relating to administrative closures. After USCIS previously raised this issue, we provided a USCIS employee with the A number associated with each error. The USCIS employee reviewed each application and told us that the policy change did not impact any error. All nine A-files with errors relating to administrative closures were completed prior to January 2024. For these reasons, we believe the January 2024 policy change would not impact the information reported here.

Recommendation 1: We recommend the Asylum Division Chief determine whether it is feasible to establish, and regularly assess compliance with, a benchmark for expected error rate during the security checks process. This analysis should identify if any specific type of error is incompatible with the integrity of the security checks process.

USCIS Response to Recommendation 1: Concur. Since 2011, the USCIS Refugee, Asylum and International Operations Directorate conducts annual quality assurance reviews on a sample of cases as previously noted in this letter. These reviews include collecting data on whether security checks are completed correctly. USCIS will consider adding further analyses to the annual review process related to security check errors and whether those errors are incompatible with the integrity of the security checks process. The Asylum Division Chief will set the error rate benchmark based upon a review and assessment of cases, as appropriate. Estimated Completion Date: December 31, 2026.

OIG Analysis: We consider this action responsive to the recommendation, which is open and resolved. We will close this recommendation when Asylum Division provides evidence of its completed analysis.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Recommendation 2: We recommend the Asylum Division Chief evaluate methods and implement changes to the [REDACTED] ★ policy and process to increase the effective identification and recordation of aliases to ensure they are processed for security checks.

USCIS Response to Recommendation 2: Concur. The Asylum Division implemented changes to guidance addressing alias identification and has implemented training to address errors identified in the OIG draft report related to missed aliases or improper alias documentation. Specifically, on December 11, 2025, Asylum Division formally incorporated the [REDACTED] ★ to the Asylum Division's " [REDACTED] ★," to provide written formal guidance on alias identification. In addition, the Asylum Division developed interactive training that defines aliases and provides detailed instructions on properly identifying and documenting aliases. This training leverages practical exercises to provide asylum personnel who conduct security checks with hands-on practice. All asylum personnel who conduct security checks must complete this training by July 15, 2026. Moreover, the Asylum Division will require that future asylum personnel who will conduct security checks also complete this training.

Building on these efforts, the Asylum Division will continue to identify and test potential solutions, including evaluating potential technical and nontechnical solutions to increase the efficiency and efficacy of alias identification. The Asylum Division plans to review local asylum office's procedures for identifying aliases and compare results with errors identified during past quality assurance reviews. The Asylum Division will analyze results, determine whether procedural changes may increase efficacy and reduce errors, and will implement changes, as appropriate. Estimated Completion Date: February 26, 2027.

OIG Analysis: We consider these actions responsive to the recommendation, which is open and resolved. We will close this recommendation when Asylum Division provides documentation of its updated training and [REDACTED] ★ and provides evidence of its completed evaluation of additional solutions to increase efficacy of alias identification.

Recommendation 3: We recommend the Asylum Division Chief identify and implement additional information system controls or other changes to ensure all required security checks are performed before an application is administratively closed.

USCIS Response to Recommendation 3: Concur. The Asylum Division will review current policies and guidance and evaluate what additional mechanisms may be implemented to ensure that required security checks are performed before it administratively closes an asylum application. On May 5, 2026, the Asylum Division implemented optional supervisory asylum officer review of administrative closures in the asylum case management system. The Asylum Division will also evaluate the effectiveness of supervisory review as a control measure to ensure required security



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

checks are performed before administratively closing an application. The Asylum Division will analyze the data to identify and implement programmatic changes to supervisory review, as appropriate. Estimated Completion Date: April 30, 2027.

OIG Analysis: We consider this action responsive to the recommendation, which is open and resolved. We will close this recommendation when Asylum Division provides evidence of its completed analysis.

Recommendation 4: We recommend the Asylum Division Chief assess whether transitioning all adjudications to an electronic [REDACTED] would improve [REDACTED] completion consistency.

USCIS Response to Recommendation 4: Concur. The Asylum Division will conduct a study to evaluate whether documenting the review of security checks electronically helps ensure that security checks are completed consistently. Specifically, USCIS will review and compare cases where the asylum officer manually recorded the review of security checks results versus cases where asylum officers recorded the review of security checks electronically in the asylum case management system. This study will evaluate whether technological advances should also be pursued as an added safeguard, and USCIS—led by the Asylum Division—will analyze the results to determine efficacies to inform changes to the Asylum Division’s security check guidance. USCIS will make results available to other USCIS program offices and directorates to inform potential policy changes relating to electronic security checks. Estimated Completion Date: April, 30, 2027.

OIG Analysis: We consider this action responsive to the recommendation, which is open and resolved. We will close this recommendation when Asylum Division provides evidence of its completed analysis.

Recommendation 5: We recommend the Asylum Division Chief identify and implement changes to ensure the Alien-file documents the asylum officer’s consideration of information identified in FDNS’ Record of Action regarding social media reviews.

USCIS Response to Recommendation 5: Concur. USCIS already commenced implementation of this recommendation. From January 2026 to April 2026, the Asylum Division conducted a thorough review of the Asylum Division’s existing policies, guidance, and procedures related to enhanced Fraud Detection and National Security Directorate review, focusing on social media policy, and existing requirements for the review, consideration, and documentation of social media results in the alien’s file. The Asylum Division drafted guidance detailing the asylum officer’s roles and responsibilities to review, consider, and properly document social media information when results are potentially derogatory, and requires the asylum officer to file a social media [REDACTED] ★ [REDACTED] which summarizes and analyzes the adjudicative impact



~~FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE~~

OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

of the social media information when Fraud Detection and National Security Directorate determines the information may be of interest. The guidance is currently going through agency review and USCIS expects to issue the final guidance in December 2026. Estimated Completion Date: December 31, 2026.

OIG Analysis: We consider this action responsive to the recommendation, which is open and resolved. We will close this recommendation when Asylum Division provides evidence of the finalized guidance.

~~FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE~~



Appendix C: **USCIS Comments on the Draft Report**

USCIS' formal management response begins on the next page.

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of the Director
Camp Springs, MD 20588-0009



U.S. Citizenship
and Immigration
Services

BY ELECTRONIC SUBMISSION

July 22, 2026

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Joseph B. Edlow
Director

SUBJECT: Management Response to Draft Report: "Adjudication Errors
in Operation Allies Welcome Asylum Files Risked
Missing Derogatory Information"
(Project No. OIG 24-015-ISP-USCIS)

Thank you for the opportunity to comment on this draft report. U.S. Citizenship and Immigration Services (USCIS) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

USCIS leadership appreciates OIG's recognition in the draft report that OIG did not observe a statistically significant increase in the error rate discussed in this report for the time period following the September 2023 *Ahmed v. DHS* settlement agreement, which mandated that USCIS adjudicate 90 percent of asylum applications from the Operation Allies Welcome population within 150 days. OIG also noted that asylum officers may be unable to entirely avoid missing aliases due to the volume of files with numerous name variations and aliases. USCIS remains committed to continuous improvement of screening, vetting, and security checks policies and procedures to ensure prompt identification, consideration, and resolution of derogatory information.

However, it is important for readers to understand that the draft report does not appear to take into consideration the fact that any instances in which asylum officers may have missed aliases or improperly documented security checks results take place amid broader, established, and robust screening, vetting, and security checks safeguards already in place that minimize the impact of these errors. Further, the draft report does not contain sufficient context to conclude that the errors were outcome determinative or indicative of derogatory information that asylum officers had not identified. The methodology utilized

Management Response to Draft Report: “Adjudication Errors in Operation Allies Welcome Asylum Files Risked Missing Derogatory Information” (Project No. OIG 24-015-ISP-USCIS)

Page 2

by the OIG appears to have focused on identifying administrative errors without conducting additional security checks or reassessing the asylum officer’s decision to determine the adjudicative impact, if any, on the cases, or whether the derogatory information actually existed in cases where the asylum officer committed these administrative errors.

The USCIS Refugee, Asylum and International Operations Directorate’s Asylum Division’s screening, vetting, and security check procedures are well-established and thorough. Asylum officers apply these requirements during their adjudication of asylum applications to identify national security threats, public safety concerns, or other derogatory information about aliens who have applied for asylum. The Asylum Division’s security check requirements include recurrent and continuous biometric and biographical checks against multiple U.S. law enforcement and watchlisting databases.

The Asylum Division also leverages technological enhancements to optimize search capabilities when conducting security checks. For example, when searching for an alien’s immigration history, prior removals, and apprehensions by Immigration and Customs Enforcement or Customs and Border Protection, the Asylum Division utilizes technology to query the alien’s A-number,¹ Fingerprint Identification Number, name(s), and date(s) of birth against multiple databases. By checking both biographic and biometric information, the Asylum Division maximizes its ability to identify derogatory information across multiple systems when conducting security checks while minimizing the impact of human errors resulting from potentially missed aliases.

USCIS also continues to enhance security check and vetting requirements for aliens who have applied for asylum. On March 1, 2024, for instance, the Asylum Division began conducting checks through the National Vetting Center. On May 1, 2025, the Asylum Division introduced continuous vetting against the DHS Watchlist Service using the Unified Passenger system. These forward-leaning enhancements provide additional layers of security to help identify potential risks throughout the asylum adjudication process. The Asylum Division automatically runs National Vetting Center and Unified Passenger system checks, and designated Fraud Detection and National Security Directorate personnel review derogatory information and prioritize cases with national security and/or public safety concerns for individualized and enhanced review. By automating and increasing the types of required security checks while expanding

¹ A-number (Alien Registration Number) is a unique identifier assigned by the U.S. Department of Homeland Security to aliens.

Management Response to Draft Report: “Adjudication Errors in Operation Allies Welcome Asylum Files Risked Missing Derogatory Information” (Project No. OIG 24-015-ISP-USCIS)

Page 3

continuous vetting, the Asylum Division continues to reinforce safeguards and to further minimize the potential impact of asylum officer errors when completing security checks.

Additionally, the USCIS Refugee, Asylum and International Operations Directorate conducts annual quality assurance reviews of asylum applications, from start to finish of the adjudications process, which includes the review of security checks, as a measure to ensure maximum adherence to policies and procedures. As corrective measures in the quality assurance review, USCIS takes an additional step to run security checks for missed aliases and to accurately complete and analyze security check results, including whether derogatory information actually existed, where USCIS identified administrative errors similar to those identified by the OIG. As a result of these efforts, USCIS unequivocally determined that any missed aliases did not impact the adjudicative outcome of any case included in USCIS’ quality assurance samples during the timeframe of OIG’s study. The Asylum Division uses the results from these quality assurance reviews to identify and correct gaps in guidance, training, and technology. For example, in fiscal year 2026, the Asylum Division formally disseminated training and guidance to asylum officers to address alias identification and documentation errors resulting from a quality assurance review.

Further, USCIS confirms that—since the period in which OIG was conducting its fieldwork for this report—the Asylum Division corrected the TECS² technical issue noted in the draft report. [REDACTED]

[REDACTED] This change likely impacted asylum applications that OIG reviewed between January 18, 2024, and February 8, 2024. However, as OIG’s draft report does not share the full list of cases reviewed, USCIS has insufficient data to validate OIG’s error determination rate related to cases administratively closed during this timeframe.

The draft report contained five recommendations, with which USCIS concurs. Attached find our detailed response to each recommendation. USCIS previously submitted technical comments addressing several accuracy, sensitivity, contextual and other issues under a separate cover for OIG’s consideration, as appropriate.

² TECS is not an acronym

**Management Response to Draft Report: “Adjudication Errors in Operation Allies
Welcome Asylum Files Risked Missing Derogatory Information” (Project No. OIG 24-015-
ISP-USCIS)**

Page 4

Thank you again for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Management Response to Draft Report: “Adjudication Errors in Operation Allies Welcome Asylum Files Risked Missing Derogatory Information” (Project No. OIG 24-015-ISP-USCIS)

Page 5

**Attachment: Management Response to Recommendations
Contained in OIG 24-015-ISP-USCIS**

OIG recommended that the USCIS Asylum Division Chief:

Recommendation 1: Determine whether it is feasible to establish, and regularly assess compliance with, a benchmark for expected error rate during the security checks process. This analysis should identify if any specific type of error is incompatible with the integrity of the security checks process.

Response: Concur. Since 2011, the USCIS Refugee, Asylum and International Operations Directorate conducts annual quality assurance reviews on a sample of cases as previously noted in this letter. These reviews include collecting data on whether security checks are completed correctly. USCIS will consider adding further analyses to the annual review process related to security check errors and whether those errors are incompatible with the integrity of the security checks process. The Asylum Division Chief will set the error rate benchmark based upon a review and assessment of cases, as appropriate. Estimated Completion Date: December 31, 2026.

Recommendation 2: Evaluate methods and implement changes to the [REDACTED] policy and process to increase the effective identification and recordation of aliases to ensure they are processed for security checks.

Response: Concur. The Asylum Division implemented changes to guidance addressing alias identification and has implemented training to address errors identified in the OIG draft report related to missed aliases or improper alias documentation. Specifically, on December 11, 2025, the Asylum Division formally incorporated the [REDACTED] to the Asylum Division’s [REDACTED] * [REDACTED] to provide written formal guidance on alias identification. In addition, the Asylum Division developed interactive training that defines aliases and provides detailed instructions on properly identifying and documenting aliases. This training leverages practical exercises to provide asylum personnel who conduct security checks with hands-

³ The [REDACTED] * [REDACTED] dated December 11, 2025, [REDACTED]
[REDACTED]
[REDACTED]

Management Response to Draft Report: “Adjudication Errors in Operation Allies Welcome Asylum Files Risked Missing Derogatory Information” (Project No. OIG 24-015-ISP-USCIS)

Page 6

on practice. All asylum personnel who conduct security checks must complete this training by July 15, 2026. Moreover, the Asylum Division will require that future asylum personnel who will conduct security checks also complete this training.

Building on these efforts, the Asylum Division will continue to identify and test potential solutions, including evaluating potential technical and nontechnical solutions to increase the efficiency and efficacy of alias identification. The Asylum Division plans to review local asylum office’s procedures for identifying aliases and compare results with errors identified during past quality assurance reviews. The Asylum Division will analyze results, determine whether procedural changes may increase efficacy and reduce errors, and will implement changes, as appropriate. Estimated Completion Date: February 26, 2027.

Recommendation 3: Identify and implement additional information system controls or other changes to ensure all required security checks are performed before an application is administratively closed.

Response: Concur. The Asylum Division will review current policies and guidance and evaluate what additional mechanisms may be implemented to ensure that required security checks are performed before it administratively closes an asylum application. On May 5, 2026, the Asylum Division implemented optional supervisory asylum officer review of administrative closures in the asylum case management system. The Asylum Division will also evaluate the effectiveness of supervisory review as a control measure to ensure required security checks are performed before administratively closing an application. The Asylum Division will analyze the data to identify and implement programmatic changes to supervisory review, as appropriate. Estimated Completion Date: April 30, 2027.

Recommendation 4: Assess whether transitioning all adjudications to an electronic [REDACTED] would improve [REDACTED] completion consistency.

Response: Concur. The Asylum Division will conduct a study to evaluate whether documenting the review of security checks electronically helps ensure that security checks are completed consistently. Specifically, USCIS will review and compare cases where the asylum officer manually recorded the review of security checks results versus cases where the asylum officers recorded the review of security checks electronically in the asylum case management system. This study will evaluate whether technological

Management Response to Draft Report: “Adjudication Errors in Operation Allies Welcome Asylum Files Risked Missing Derogatory Information” (Project No. OIG 24-015-ISP-USCIS)

Page 7

advances should also be pursued as an added safeguard, and USCIS—led by the Asylum Division—will analyze the results to determine efficacies to inform changes to the Asylum Division’s security check guidance. USCIS will make results available to other USCIS program offices and directorates to inform potential policy changes relating to electronic security checks. Estimated Completion Date: April 30, 2027.

Recommendation 5: Identify and implement changes to ensure the Alien-file documents the asylum officer’s consideration of information identified in [Fraud Detection and National Security Directorate]’s Record of Action regarding social media reviews.

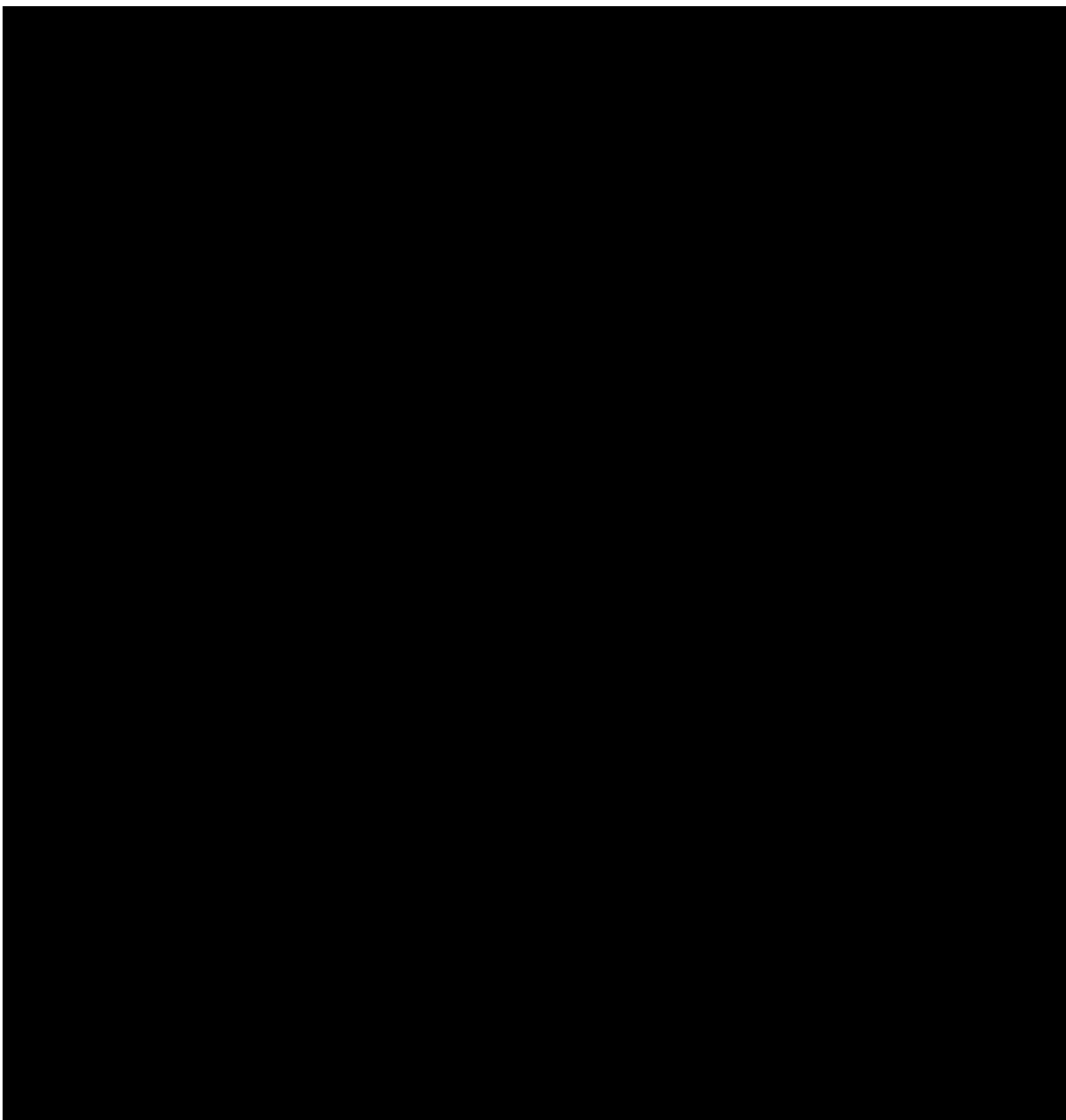
Response: Concur. USCIS already commenced implementation of this recommendation. From January 2026 to April 2026, the Asylum Division conducted a thorough review of the Asylum Division’s existing policies, guidance, and procedures related to enhanced Fraud Detection and National Security Directorate review, focusing on social media policy, and existing requirements for the review, consideration, and documentation of social media results in the alien’s file. The Asylum Division drafted guidance detailing the asylum officer’s roles and responsibilities to review, consider, and properly document social media information when results are potentially derogatory, and requires the asylum officer to file a social media [REDACTED] * [REDACTED] which summarizes and analyzes the adjudicative impact of the social media information when Fraud Detection and National Security Directorate determines the information may be of interest. The guidance is currently going through agency review and USCIS expects to issue the final guidance in December 2026. Estimated Completion Date: December 31, 2026.



Appendix D:

★

Process Diagram



Source: OIG analysis based on asylum application review



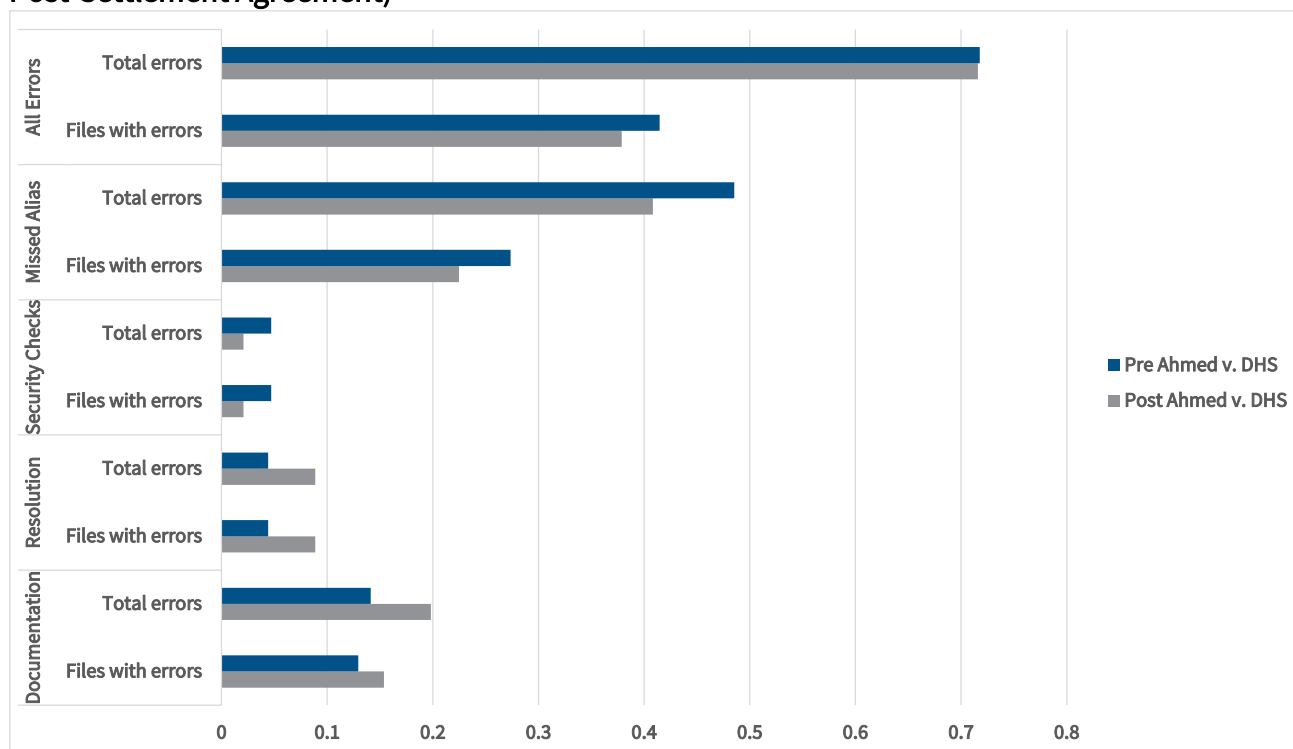
OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix E: Statistical Analysis

As shown in Figure 4, our application review resulted in pre-statistical analysis observations. We made 10 types of observations and for each observation, we paired pre- and post-settlement agreement application review results. These results showed that for all errors, the total errors and the rates of errors per file were slightly lower in the post-settlement sample. They also showed that for resolution errors and documentation errors, both the average errors per file and the prevalence of files with errors were higher in the post-settlement sample. Finally, the results showed that error rates were higher in the pre-settlement sample for security checks and missed aliases.

Figure 4. Observed Average Number of Errors and Proportion of Files with Errors (Pre- and Post-Settlement Agreement)



Source: OIG analysis

We then performed statistical analysis to infer error rates for the entire population of OAW applicants meeting our criteria. Figure 5 depicts the results of our statistical analysis. Based on this analysis, we found that missed aliases and incomplete resolution of potential matches to derogatory records did not increase following the settlement agreement, even for the observations showing higher error rates in the post-settlement agreement sample.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Figure 5 depicts with blue bullets observations from our sample of error rates post-settlement agreement subtracted from observations from our sample of error rates pre-settlement agreement. When the blue bullet is a negative value, it indicates we observed more errors after the settlement. As described above, we observed more errors in the post-settlement sample four times. Therefore, there are four bullets less than zero. The horizontal line with an arrow pointing from each blue marker depicts values that would be possible at the 95 percent confidence level when inferring observations from our sample across the entire population of OAW applications. An observation from our sample that errors increased post-settlement agreement would only be statistically significant if the entire inference line is less than zero. Because this is not the case for any of our observations, we determined that errors did not increase post-settlement agreement.

Figure 5 also presents the results of our hypothesis testing for each error type, expressed as p-values.⁶⁴ Each p-value is based on observations from our sample. We also determined a p-value at which an observation from our sample would be statistically significant. We established this p-value at 0.0062, corresponding to a 95 percent family-wise confidence level. Although two error types had relatively small p-values of 0.0068 and 0.0073, these p-values still exceed the threshold p-value of 0.0062 percent for statistical significance. We therefore determined that errors did not increase post-settlement agreement.

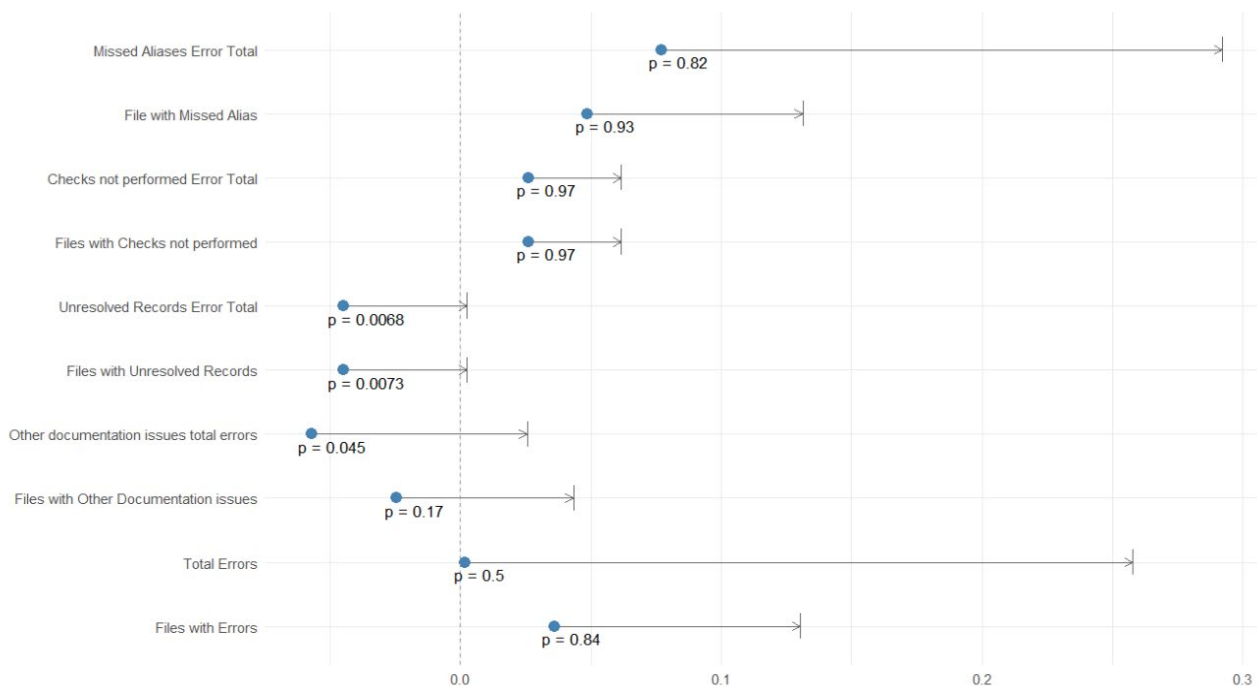
⁶⁴ A hypothesis test uses sample data to evaluate evidence about a population. The test calculates a p-value under the assumption that the null hypothesis is true. In our case, the null hypotheses are that pre-settlement error rates are equal to or greater than post-settlement error rates. When the null hypothesis is rejected due to a low p-value, then the alternative hypothesis is accepted. The alternative hypotheses in our case are that the post-settlement error rates are greater than the pre-settlement error rates.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Figure 5. Observed Differences Between Pre- and Post-Settlement Agreement Errors at a 95 Percent Confidence Level



Source: OIG analysis



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

**Appendix F:
Report Distribution**

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
USCIS Component Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, please visit our website: www.oig.dhs.gov.

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.



DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline.

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

U.S. Mail:
Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive SW
Washington, DC 20528-0305