

**U.S. CITIZENSHIP AND IMMIGRATION SERVICES**  
**National Security and Records Verification Directorate**  
**Fraud Detection and National Security Division**

**I-589 Asylum Benefit Fraud and Compliance Assessment Report**



November 16, 2009

--- FOR INTERNAL DISCUSSION ONLY ---

## *Executive Summary*

The U.S. Asylum Program provides the opportunity for applicants who meet the definition of a refugee<sup>1</sup> and have arrived in the United States or traveled to a U.S. port of entry, to apply for legal status to remain in the U.S. Because applicants for asylum may have difficulty fleeing with or retrieving documentary evidence, credible testimony alone may be sufficient evidence to establish eligibility. Some argue that the rules regarding submission of corroborating evidence may open the Asylum Program to increased fraudulent filings. To help address this concern, USCIS conducted a Benefit Fraud and Compliance Assessment (BFCA) to study the scope and types of fraud associated with the Form I-589, *Application for Asylum and Withholding of Removal*, to determine the relative utility of a number of fraud detection methods, and to assess the extent to which the fraud detection measures that were part of the adjudication process at the time of adjudication were being utilized by Asylum Officers (AOs).

USCIS studied a sample of asylum applications that were affirmatively filed<sup>2</sup> between May 1, and October 31, 2005. All cases included in this BFCA were subject to a set of fraud detection methods, including verifying information in the applicant's file against several other U.S. and Canadian government systems.<sup>3</sup> In some cases where information or documents were suspected to be fraudulent, documents and/or facts from the case were sent overseas to U.S. government officials to verify authenticity (referred to as "Overseas Verification Requests" or "OVRs").

For the purposes of the BFCA, a case was classified as fraudulent (labeled "proven fraud") if reliable evidence pertaining to the applicant's asylum eligibility proved a material misrepresentation and the evidence was more than contradictory testimony given by the applicant.<sup>4</sup> If indicators of fraud existed and pertained to the applicant's asylum eligibility, but fraud could not be confirmed by evidence external to the applicant's testimony, the case was classified as exhibiting "indicators of possible fraud." The cases that did not present any indicators of fraud were classified as not fraudulent (labeled "no fraud").

Because USCIS did not receive responses back on all of the OVRs sent in connection with this study, USCIS had to complete its analysis with some missing data. As a result, this study can neither provide a definite estimate of fraud in the asylum program, nor

---

<sup>1</sup> The term "refugee" means any person who is outside any country of such person's nationality or, if in the case of a person having no nationality is outside any country in which such person last habitually resided, and who is unable or unwilling to return to, and is unable or unwilling to avail himself or herself of the protection of, that country 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. The term "refugee" does not include any person who ordered, incited, assisted, or otherwise participated in the persecution of any person on account of race, religion, nationality, membership in a particular social group, or political opinion. INA Section 101(a)(42).

<sup>2</sup> The definition of affirmatively filed applications, *Infra* at note 6.

<sup>3</sup> Canadian checks were performed on all but eleven cases which lacked fingerprints. Fingerprints are required to run the Canadian system checks.

<sup>4</sup> The definition of fraud is discussed in greater detail in Section 1, "Background."

report a margin of error. Rather, this report presents a detected fraud rate, indicating that if FDNS had additional fraud detection tools or received responses to all of the overseas document verification requests, the rate of proven fraud might be higher. The detected fraud rate in the asylum program for the population from which the sample was drawn is 12%.<sup>5</sup> The true fraud rate is unknown, and “fraud rate” in this report refers to the rate of “detectable” fraud. This includes fraud detected through systems checks, admissions of fraud, and/or overseas document verification.

In 12 of the proven fraud cases, asylum had been granted prior to the BFCAs. In these cases, the BFCAs yielded information that would not have been obtained in the normal course of the adjudications under procedures in place at the time that the cases were completed. For each of these 12 cases, the Asylum Program initiated terminations proceedings based on the results of the study. The identification of proven fraud cases through the application of the additional fraud detection methods used in the BFCAs demonstrates the value of those fraud detection tools.

Among the cases determined by this review to be proven fraud, there were no instances where an asylum office granted a case and failed to properly complete the mandatory background and security check procedures in place at the time of the adjudication. In all cases, AOs completed security checks and correctly recorded results in accordance with Asylum Program requirements. As one objective of the BFCAs to assess the extent to which fraud detection measures were part of the adjudication, these results indicate that the Asylum Program employed required fraud detection measures to the fullest extent possible in each of these adjudications.

In this study, the majority of the cases, 58% (138/239), exhibited indicators of possible fraud, and 30% (72/239) of cases contained no fraud. Of the cases with indicators of possible fraud, 76% (105/138) were referred to an Immigration Judge independent of the BFCAs. The high rate of referral of these cases indicate that current techniques and procedures that the Asylum Program utilizes in adjudicating cases are reasonably effective in dealing with cases that contain indicators of fraud.

Each of the fraud detection methods utilized in this BFCAs confirmed a finding of proven fraud in at least one case. Overseas document verification was the most successful method employed because it provided definitive evidence of fraud for the largest number of proven fraud cases (17 out of 29). U.S. Government system checks yielded evidence of fraud in seven (7/29) proven fraud cases; Canadian immigration system checks supported findings in three (3/29) cases; and commercial data broker checks provided the evidence in one (1/29) case. In addition, there was one (1/29) case in which the applicant’s admission of fraud pursuant to an ICE investigation led to a finding of proven fraud, demonstrating the valuable role that ICE can play in pursuing cases where fraud is suspected.

---

<sup>5</sup> The margin of error for this point estimate would have been  $\pm 4.1\%$  if the entire sample had been subjected to overseas verification requests.

As a result of this study, USCIS intends to publish internal recommendations to aid the asylum adjudication processes.

DRAFT

## Table of Contents:

1.	<b>Background</b>	6
	A. The BFCFA Program	6
	B. The U.S. Asylum Program	7
2.	<b>The Study Population</b>	9
3.	<b>Methodology</b>	9
	A. Systems Checks	10
	B. Overseas Document Verification	10
	C. Definitions of Fraud Categories	11
4.	<b>Key Findings</b>	11
	A. 12% of Asylum Cases Found to be Proven Fraud	12
	B. 58% of Asylum Cases Contained Indicators of Possible Fraud	12
	C. 30% of Asylum Cases Contained No Fraud	13
5.	<b>Analysis of Proven Fraud Cases</b>	13
	A. Asylum Officers Correctly Followed All Established Security Check Procedures <i>Integrity Standards Upheld</i>	14
	B. The Effectiveness of Each Fraud Discovery Method	14
	C. Analysis of the Data Revealed No Discernable Trends Across Several Variables	21
6.	<b>Indicators of Possible Fraud Analysis</b>	21
	A. AOs Referred to Immigration Courts 54% of the Cases Identified as having Indicators of Possible Fraud Based on a Negative Credibility Determination	21
	B. 10% of Cases Contained a Pattern of Fraud Under Asylum Office/FDNS Monitoring	22
	C. 9% of Cases Involved Individuals Under Investigation	22

D. Other	23
<b>7. Actions Taken Since the BFCA</b>	<b>23</b>
A. US Government Systems Checks	23
B. Information Sharing with Other Countries	23
C. Overseas Document Verification	24
D. Additional Support for Investigation and Prosecution of Immigration Service Providers that Facilitate and Profit from Asylum Fraud	24
<b>8. Recommendations</b>	<b>25</b>
<b>9. Conclusion</b>	<b>25</b>
<b>Appendix</b>	<b>26</b>

DRAFT

## ***1. Background***

USCIS conducted this BFCA for three purposes. The first and primary purpose was to conduct a study on the scope and types of fraud associated with the Form I-589, *Application for Asylum and Withholding of Removal*. The second purpose was to determine the relative utility of a number of fraud detection methods. The third purpose was to assess the extent to which the fraud detection measures that were part of the adjudication process at the time of adjudication were being utilized by Asylum Officers (AOs).

For the purposes of the BFCA, fraud is defined as a willful misrepresentation or falsification of a material fact. Fraud entails any manifestations that amount to an assertion not in accordance with the facts, an untrue statement or concealment of a material fact, or an incorrect or false representation material to asylum eligibility.

This document describes the methodology used to measure fraud within the Asylum Program and the results of the application of those methods. This section provides an overview of the history of the BFCA program and a description of the U.S. Asylum Program. The next two sections describe the BFCA program and provide an overview of the Asylum Program and the skills and resources Asylum Officers and FDNS Immigration Officers use to identify fraud. The section entitled “Study Population” explains the sample population and how it was identified. The “Methodology” section describes the methods that FDNS Immigration Officers used to identify fraud within the sample population applications and how cases were ultimately classified for purposes of this study. The overall fraud rate, overseas verification results, and the effectiveness of fraud detection methods are discussed in the “Key Findings and Analysis” section. The “Actions Taken Since the BFCA” section describes steps taken since the time of the study to enhance the integrity of the Asylum Program.

### ***A. The BFCA Program***

The Government Accountability Office (GAO) Report 02-66, entitled *Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems*, issued on January 31, 2002, found that the United States’ legal immigration system was being abused and potentially used to threaten national security, public safety, and commit other illegal activities, such as human and narcotics trafficking. The GAO Report indicated that legacy INS needed to: 1) implement a sound anti-fraud benefit strategy, 2) designate detection of immigration benefit fraud as a priority initiative, and 3) create a mechanism to collect and report data to identify the volume and scope of immigration benefit fraud that exists.

In May 2004, U.S. Citizenship and Immigration Services (USCIS) responded to the concerns raised in the GAO report and national security and public safety needs by creating the Office of Fraud Detection and National Security (FDNS) as the foundation upon which to build its fraud detection and prevention effort. In February 2005, FDNS

developed and implemented a Benefit Fraud Assessment (BFA) program, later renamed the Benefit Fraud and Compliance Assessment (BFCA) program, to measure the integrity of specific nonimmigrant and immigrant applications and petitions by conducting administrative inquiries on randomly selected cases. Although the name of the program has changed to reflect the full range of issues reviewed, the methodology used to conduct the assessments has not changed. The applications and petitions reviewed are not selected because they are suspected of fraud, but are a sampling of pending and completed cases over a recent six-month period. The results of the BFCA serve as a basis for proposed changes to existing regulations, policies, and procedures, and as warranted, recommended legislative remedies.

While conducting these assessments, FDNS analyzes the scope of an immigration program for fraud vulnerabilities. Information gleaned from a BFCA may aid USCIS in further developing fraud detection and prevention strategies, establish priorities for workload planning purposes, and inform fraud pattern and linkage data for case referral to Immigration and Customs Enforcement (ICE) or closer examination by adjudicating officers.

In keeping with the USCIS/ICE anti-fraud joint strategy,<sup>6</sup> USCIS may refer some or all of the BFCA cases with preliminary findings of fraud to ICE for criminal investigation, possible prosecution, and removal, if warranted. In addition, the USCIS component with authority over the adjudication process is informed of all findings of fraud so that the component can take appropriate administrative actions on the specific case findings such as denial, referral, revocation, and/or termination of benefits. All BFCA cases are entered into the FDNS Data System (FDNS-DS) for tracking and case management purposes. Suspected fraud disclosed during a BFCA is entered into FDNS-DS as either a lead or case and is accessible by FDNS officers and ICE agents conducting administrative and criminal investigations.

### ***B. The U.S. Asylum Program***

Asylum is a government-granted form of protection provided to foreign nationals who were persecuted or have a well-founded fear of persecution in their country on account of their race, religion, nationality, membership in a particular social group, or political opinion. The U.S. Asylum Program provides this status to qualified applicants who have already entered the United States or are seeking entry to the U.S. at a port of entry.

In an affirmative asylum adjudication, the applicant generally has the burden of proving that he or she: 1) is eligible to apply for asylum status, 2) is a refugee within the meaning of section 101(a)(42)<sup>7</sup> of the Immigration and Nationality Act (INA), 3) is not statutorily barred from a grant of asylum, and 4) merits asylum as a matter of discretion.<sup>8</sup> To fulfill

---

<sup>6</sup> See Attached Memorandum of Understanding with Immigration and Customs Enforcement dated September 2008.

<sup>7</sup> Definition of Refugee, *Supra*, at 1.

<sup>8</sup> Every grant of asylum to an individual who establishes refugee status is discretionary. If it is determined that an applicant is eligible for asylum, there must also be a determination that an applicant merits a



this burden, the applicant must present testimony that is credible, persuasive, and specific. The applicant may also furnish documentary evidence; however, due to the emergent circumstances that may be associated with refugee flight, asylum applicants are not required to submit corroborating documentation when such items cannot be reasonably obtained. For these reasons, section 208(b)(1)(B)(ii) of the INA states that credible testimony alone may be sufficient to establish asylum eligibility.

Although documentary evidence is not required, in the majority of asylum cases, applicants submit documents to prove their identity and/or meet their evidentiary burden to establish asylum eligibility. For example, they may submit passports and national identity documents to establish identity. Examples of evidence submitted to support the asylum claim include documents issued by law enforcement authorities, medical facilities, employers, political and religious organizations, and other civil authorities, as well as country condition information relevant to their claim for protection.

An asylum applicant's use of a fraudulent document does not necessarily constitute fraud in the overall asylum claim and might not affect his or her eligibility for asylum status. For example, an applicant may obtain a fraudulent travel document to flee the country of feared persecution and travel to the United States. If the applicant discloses to the Asylum Officer that the document is fraudulent and provides a plausible explanation for using it, his or her use of the fraudulent document may ultimately support the claim rather than adversely impact eligibility. Thus, the facts and circumstances of each asylum case must be considered in the determination of whether fraud is material to an asylum claim. All FDNS Immigration Officers (IOs) and Asylum Officers (AOs) are trained to analyze documents to determine whether a document exhibits indicators that it is counterfeit, altered, or was issued to an individual other than the individual presenting the document. In addition, passports, national ID cards, and other commonly issued documents may be sent to the Immigration and Customs Enforcement Forensic Document Laboratory (ICE FDL) for analysis and a determination regarding authenticity. While these resources have helped the Asylum Program to more effectively identify and address document fraud, asylum applicants may present a wide range of official, semi-official, and/or unofficial documents from overseas locations, making document fraud determinations an ongoing challenge.

AOs are required to conduct an analysis of credibility and make a credibility determination in each case that they adjudicate. In doing so, AOs consider such factors as: 1) the accuracy, truthfulness, and consistency of the statements provided between and within the oral and written testimony, 2) the sufficiency of detail provided by the applicant, 3) the inherent plausibility of the facts alleged by the applicant, and 4) the demeanor, candor, and responsiveness of the applicant. A negative credibility finding alone, however, does not necessarily demonstrate asylum fraud; it may reflect the

---

favorable exercise of discretion. 8 C.F.R. Section 208.14(b) indicates that an asylum officer may grant, in the exercise of his or her discretion, asylum to an applicant who qualifies as a refugee under INA Section 101(a)(42).

applicant's inability to provide sufficiently credible testimony to meet his or her burden of proof.

## **2. *The Study Population:***

The population from which the data was drawn for this study included asylum applications that were filed between May 1, and October 31, 2005, and that received final adjudication or were still pending as of January 2006. The study was also limited to asylum applications within the jurisdiction of USCIS that were filed affirmatively<sup>9</sup> at USCIS Service Centers or directly with Asylum Offices. The Asylum BFCAs did not include asylum applications filed defensively with the Department of Justice, Executive Office for Immigration Review (EOIR). This population totaled 8,555 asylum applications. The sample size of 239 applications was selected for the purpose of estimating the overall detectable fraud rate with a 95% confidence interval, an intended margin of error of  $\pm 5\%$ , and assuming a 20% rate of occurrence.<sup>10</sup> The 239 applications in the BFCAs were randomly pulled from the Refugee, Asylum, and Parole System (RAPS) database regardless of Asylum Office jurisdiction or any other demographic stratification. The principal applicants of the 239 BFCAs cases represented applicants from over 50 nationalities. The countries of nationality that had the highest representation were China (55 applicants), Haiti (21 applicants), Colombia (21 applicants), and Mexico (14 applicants).

## **3. *Methodology:***

Fraud Detection and National Security Immigration Officers (FDNS IOs) located in each of the eight Asylum Offices conducted the first stage of this study. FDNS IOs performed a standard battery of system checks on every case. FDNS IOs reviewed all material in the applicants' A-files, T-files, working files, and related electronic case management records.

Once system checks and a review of the file were completed and no documents were identified as warranting overseas verification, a final determination was made. In many

---

<sup>9</sup> An alien seeking asylum in the United States can apply either affirmatively or defensively, depending on his or her circumstances. When filing affirmatively, an asylum-seeker files Form I-589, *Application for Asylum and Withholding of Removal*, with the appropriate USCIS Service Center or Asylum Office within one year of his or her last arrival in the United States (unless an exception to the one-year rule applies). An asylum-seeker files defensively in Immigration Court before an Immigration Judge (IJ) by filing Form I-589, *Application for Asylum and Withholding of Removal*, as a defense against removal from the United States. An asylum-seeker who does not establish eligibility for asylum affirmatively will, if not in a legal immigration status, be referred to Immigration Court where he or she can again apply to establish eligibility for asylum before an IJ.

<sup>10</sup> This random sampling formula was provided and approved by the DHS Office of Immigration Statistics (OIS). Because there were no estimates of fraud available within the asylum population from previous studies, OIS recommended a simple random sample of cases for this study. The sample design used in this study is similar to that used in other BFCAs.

cases, if information or documents were suspected to be fraudulent and it was believed that consultation with overseas sources could confirm or refute the suspicion, an overseas verification request was submitted. Once the overseas verification request was returned, a final determination was made. After the FDNS IOs conducted their reviews and analyses, Headquarters staff conducted the second stage reviews of each determination to ensure that the primary determinations were consistent among FDNS IOs in all field asylum offices. For cases in which no OVR response was received, a determination was made based on available information.

### **A. System Checks**

FDNS IOs conducted government system and commercial data broker checks on all subjects in the BFCA, including applicants, dependents, interpreters, preparers, and representatives.<sup>11</sup> These checks were conducted to identify possible fraud indicators associated with information contained in the asylum application. These checks included an up-to-date inquiry of all government systems that are required in the adjudication of an asylum case, as well as additional systems that were not required at the time of adjudication. FDNS IOs then reviewed the system checks to determine whether the records they found were consistent with the information that the applicant provided during the asylum adjudication.

The Asylum Division may exchange information with Canada on individual asylum cases to confirm elements of asylum eligibility. As part of this study, biometrics of the BFCA principal applicants<sup>12</sup> and their dependents were checked against Canadian immigration systems to determine whether the subjects previously applied for refugee status in Canada. In cases where a search of these databases yielded a biometric match, the specific case information obtained was used to verify the credibility of the applicant's testimony in support of his or her U.S. asylum claim.

### **B. Overseas Document Verification**

After conducting the systems checks and file review described above, FDNS IOs could request overseas verification of the authenticity of the supporting documents or facts claimed by applicants. Because of the time and resource requirements of overseas verification, cases were sent when there were specific reasons to believe that there would be relevant information obtained overseas and there was insufficient evidence to otherwise substantiate a fraud finding.

OVRs were submitted in 59 of the 239 BFCA cases. The documents that were submitted for overseas verification were sent to the USCIS Office of International Operations

---

<sup>11</sup> Interpreters and preparers were checked against Central Index System and to Commercial Databases (CDBs). If there was adverse information found about an interpreter or preparer from another source (for example, an interpreter being on an office's "banned interpreter list"), that information was noted by the FDNS IO. Attorneys/representatives were checked against RAPS, DHS/DOJ records regarding disbarred or disciplined attorneys, and state bar and/or consumer protection bureau records.

<sup>12</sup> Eleven applicants did not receive the Canadian check due to the unavailability of fingerprints required to run the check.

whenever possible. In countries that lacked a USCIS presence, the documents were sent to the U.S. Department of State, Bureau of Democracy, Human Rights and Labor.

**C. Definitions of Fraud Categories:** After review of all information obtained through systems checks, file review, and OVRs, the FDNS IO determined whether the case exhibited *proven fraud, indicators of possible fraud, or no fraud*.

**(i) Proven Fraud:** A case was determined to contain proven fraud when a fraud indicator material to asylum eligibility was confirmed by reliable evidence external to the applicant's testimony and could be clearly articulated in the written explanation of the BFCAs case findings.

**(ii) Indicators of Possible Fraud:** A case was determined to contain indicators of possible fraud when indicators of fraud material to asylum eligibility were present (e.g., material inconsistencies between testimony and written statements) but could not be confirmed by sufficient reliable evidence external to the applicant's testimony. This category included cases where there was a pre-identified pattern of claim subject to internal monitoring.<sup>13</sup> It also included cases where no substantiated external fraud indicators were found, but an immigration service provider (preparer, interpreter, and/or attorney/representative) associated with the case was convicted of immigration fraud or was currently under investigation for immigration fraud. An AO's negative credibility determination, for this study's purpose, was treated as an indicator of possible fraud because the determination was based upon a material inconsistency in the testimony or associated with a lack of accuracy or truthfulness in the statements provided.

**(iii) No Fraud Indicators:** A case was determined to be in this category when it exhibited no indicators of fraud material to asylum eligibility.<sup>14</sup>

For cases determined to exhibit proven fraud or indicators of possible fraud, FDNS IOs also reviewed the case to determine whether the Asylum Officer identified the fraud indicator when adjudicating the case.

#### **4. Key Findings:**

The results of the BFCAs yielded a detected fraud rate of 12%<sup>15</sup> (29/239).<sup>16</sup> This includes fraud detected through systems checks, admissions of fraud, and overseas document

---

<sup>13</sup> Further information regarding fraud patterns subject to monitoring, *Infra* at 18.

<sup>14</sup> Other types of fraud or system abuse/misuse may have been identified, but the focus of the BFCAs was to identify asylum fraud indicators and determine the extent of asylum fraud in the sample population. Examples of non-asylum system abuse include fraud related to social security, family-based petitions, and jurisdiction (i.e. misrepresenting an address to file in one asylum office over another).

<sup>15</sup> The margin of error for this point estimate would have been  $\pm 4.1\%$  if the entire sample had been subjected to overseas verification requests.

<sup>16</sup> For a more complete understanding, 12% should be thought of in two parts: 5% ( $\pm 2.8\%$ ) is the fraud rate detected through system checks and admission of fraud. The other portion of the detectable fraud rate is the fraud detected by overseas verification, which is at least 7%.

verification. Additionally, 30% (72/239) of cases contained no fraud. Finally, recognizing the unique nature of asylum claims as particularly dependent on the applicant's testimony alone and the limitations of the government's ability to independently verify the unique facts of the claim, the methodology included an intermediate category, "indicators of possible fraud," to capture those cases where USCIS identified indicators of possible fraud that could not be independently verified. In this study, 58% (138/239) of cases exhibited indicators of possible fraud. Of the cases in the study that were found to have proven fraud or indicators of possible fraud, 72% (121/167) were referred to an Immigration Judge independent of the BFCAs.

The results of the study are limited due to lack of response to 33 overseas verification requests. Of the 239 applications in the sample, the analysis of 206 cases was based on all requested information.<sup>17</sup> The remaining 33 cases are those without a response to the OVR and were given a BFCAs fraud classification based on the information available. Given that limitation, this study provides a detectable fraud rate with the understanding that additional information on 33 cases would likely yield a higher detected fraud rate. Assessing the information available for these 33 cases, 6 were determined to have no fraud, and 27 were determined to have indicators of possible fraud. While the 6 cases with no fraud were found by FDNS IOs to warrant closer review of the documents submitted, upon further review, the evidence presented did not meet the standard for the final determination of *indicators of possible fraud*.

#### **A. 12% (29/239) of Asylum Cases Found to be Proven Fraud:**

A total of 29 out of 239 (12%) cases were classified as "proven fraud." The rate of proven fraud discovered in the sample through system checks and admission of fraud was 5% (12/239). Overseas verification proved fraud in 7% (17/239) of all cases. In 12 of the 29 proven fraud cases, or 5% (12/239) of the overall population, asylum had been granted prior to the BFCAs. These 12 cases are significant because they represent instances in which applicants successfully perpetrated fraud and obtained the asylum benefit. In these cases, the BFCAs yielded information that would not have been obtained in the normal adjudicative process under procedures in place at the time that the case was completed. For each of these 12 cases, the Asylum Program initiated terminations proceedings based on the results of this study. In 11 cases, asylum status was terminated. In the remaining case, severe medical conditions prevent the applicant from appearing before USCIS in termination proceedings. The identification of proven fraud cases through the application of the additional fraud detection methods used in the BFCAs demonstrates the value of those fraud detection tools.

#### **B. 58% (138/239) of Asylum Cases Contained Indicators of Possible Fraud:**

FDNS concluded that there were 138 cases with indicators of possible fraud (111 cases that were completed based on all requested information and 27 of the 33 cases that did not receive an overseas verification result), meaning that 58% (138/239) of the study's cases exhibited indicators of possible fraud. Of these cases, 22% (30/138) were approved

---

<sup>17</sup> In 26 of the 206 cases the requested information included the results of an OVR.

prior to the completion of the BFCAs and 78% (108/138) were referred to an immigration judge.<sup>18</sup>

There were 34 cases in which the indicator of possible fraud was, at least in part, a fact or document submitted by the applicant that the FDNS IO determined should be sent for overseas verification. In 7 of these 34 cases, USCIS received the response to the overseas verification request, but the results were insufficient to support a finding of proven fraud. The remaining 27 cases are those that did not receive an overseas verification response, and the fraud classification of “indicators of possible fraud” was based on all other evidence available, including consideration of the initial concerns that led to the document being sent overseas.

**C. 30% (72/239) of Asylum Cases Contained No Fraud:**

The remaining 30% (72/239) of the cases contained no fraud indicators. Cases in this category did not exhibit any indicators of fraud material to asylum eligibility. Out of the cases in this category, 42% (30/72) were approved and 58% (42/72) were referred or denied due to statutory ineligibility or discretionary factors.

See **Table 1** for the final adjudications on the sampled cases. Asylum was granted in 30% (72/239) of the cases and 70% (167/239) of the cases were referred or denied.

**Table 1. Final Adjudicative Decisions and Fraud Classifications of Completed BFCAs Asylum Cases**

Final Adjudicative Decision	Proven Fraud Cases	Indicators of Possible Fraud	No Fraud	Total Cases
Approved	12 (5%)	30 (13%)	30 (13%)	72 (30%)
Not Approved <sup>‡</sup>	17 (7%)	108 (45%)	42 (18%)	167 (70%)
<b>Total</b>	<b>29 (12%)</b>	<b>138 (58%)</b>	<b>72 (30%)</b>	<b>239</b>

<sup>‡</sup>This category comprises both referrals to the Immigration Court and asylum denials.

**5. Analysis of Proven Fraud Cases:**

To assess the integrity methods implemented in the Asylum Program, this study analyzed whether the method by which the “proven fraud” had been identified was either: 1) a measure that was required at the time of adjudication but not properly applied by the adjudicating officer; 2) a measure that was not required at the time of adjudication but is now required; or 3) a measure that was not required at the time of adjudication and is not presently required in asylum adjudications.

<sup>18</sup> Denials are issued for applicants who maintain a legal immigration status at the time of the asylum decision. Applicants who are found not eligible for asylum and do not have a legal immigration status at the time of the decision are referred to the Immigration Judge.

### **A. Asylum Officers Correctly Followed All Established Security Check Procedures - *Integrity Standards Upheld***

Among the cases determined by this review to contain proven fraud, there were no instances where an AO granted a case and failed to properly complete the mandatory background and security check procedures in place at the time of the adjudication. In all cases, AOs completed security checks and correctly recorded results in accordance with Asylum Program requirements. One case was found to have “proven fraud” through a measure that was not required at the time of adjudication, but is required under present procedures. In the remaining “proven fraud” cases, the fraud was discovered using methods that were not mandatory at the time of adjudication and, though employed on a case-by-case basis today, are not required at the present time. In addition, through the repeated security checks performed for the BFCA, there was no case identified that involved national security concerns.

### **B. The Effectiveness of Each Fraud Discovery Method**

In the majority of the proven fraud cases (17/29, or 59%), overseas document verifications provided the evidence supporting the finding. Each of the other fraud discovery methods identified fraud to some degree. In 24% (7/29) of proven fraud cases, U.S. Government system checks yielded evidence of fraud; Canadian immigration system checks supported findings in 10% (3/29) of the proven fraud cases<sup>19</sup>; and commercial data broker checks provided the evidence in one (4%) of the 29 proven fraud cases. In addition, the applicant’s admission of fraud pursuant to an ICE investigation led to a finding of proven fraud in one case (4%).

#### ***(i) US Government Systems Checks Confirmed Fraud in 24% (7/29) of the Proven Fraud Cases:***

INA section 208(d)(5)(A)(i) states that asylum cannot be granted until the identity of the applicant has been checked against all appropriate records or databases maintained by the Attorney General and the Secretary of State. Congress added this provision to ensure that all appropriate resources were checked to determine whether the applicant is ineligible for benefits and/or if there are any grounds on which the alien may be inadmissible to or removable from the United States. USCIS has instituted numerous mandatory biographical and biometric checks for all asylum applicants and has consistently employed newly available technologies to augment its security check procedures. The results of all security and background checks must be received and reviewed prior to a grant of asylum.

Additionally, as part of this BFCA, FDNS IOs utilized other non-mandatory systems checks to investigate fraud in the sample. Non-mandatory system checks that produced

---

<sup>19</sup> Because 11 cases did not receive Canadian checks due to a lack of fingerprints, it is possible that more fraud or indicators of proven fraud would have been discovered.

fraud information include: SEVIS, IBIS (SQVS),<sup>20</sup> IBIS (SQ94), IBIS (SQPQ), IBIS (SQAD), Accurint, (Commercial), Auto Track (Commercial), ADIS, and SC CLAIMS.

***(a) DHS US-VISIT<sup>21</sup> (1/7 Cases Where U.S. Government Systems Checks Confirmed Proven Fraud):***

US-VISIT provides information drawn from Customs and Border Protection (CBP) Form I-94, Arrival and Departure Records linked to biometric data. In 2004, CBP inspectors began capturing biometrics of non-immigrants arriving at certain airports and ports of entry in the US-VISIT database. Although exceptions do apply, one of the requirements to qualify for asylum status is that the individual applies within a year of his or her last arrival to the United States. Therefore, for the purposes of evaluating the applicant's eligibility and detecting asylum-related fraud, it is important to verify date of entry into the U.S. At the time of the BFCAs, US-VISIT was not a mandatory system check; however that changed as of May 2006.

In one BFCAs case, US-VISIT produced information that supported a finding of proven fraud. The check indicated an applicant's arrival to the U.S. in 2001; however, there were no departure data found in any other systems. The applicant testified in her asylum application that she entered without inspection in January 2005. In this case, the applicant's actual date of entry as recorded in US-VISIT predated the period when DHS began capturing non-immigrant arrivals into the system. FDNS accessed older I-94 records to confirm the earlier arrival, which was instrumental in yielding entry information and identifying the discrepancy regarding the applicant's claimed date of arrival. Through this case, US-VISIT which was not a required check at the time the case was adjudicated, was confirmed as an effective fraud detection method.

***(b) Department of State (DOS) Consular Consolidated Database (CCD) (3/7 Cases Where U.S. Government Systems Checks Confirmed Proven Fraud):***

In the BFCAs, CCD was useful in detecting asylum-related fraud as it provided FDNS access to information from the DOS adjudication of visa applications. This allowed the IOs to compare the visa adjudication information with information provided in the asylum application and to address any apparent inconsistencies and other issues related to obtaining a visa. While misrepresentation to a State Department Consular Officer to obtain a visa to flee to the U.S. does not necessarily adversely affect asylum eligibility and may even support the applicant's asylum claim, it is nonetheless important for AOs to have that information, which equips them with the ability to determine whether this type of misrepresentation is material to asylum eligibility. Asylum Officers could not

---

<sup>20</sup> At the time of the BFCAs, IBIS (SQ11) was the only required IBIS check prior to a grant of asylum.

<sup>21</sup> US-VISIT is the acronym for United States Visitor and Immigration Status Indicator. Note that prior to May 2006 it was mandatory for Asylum Officers to complete a biometric check against US-VISIT's predecessor system IDENT. That system provided checks against the Asylum biometric database, as well as databases for watchlist cases and recidivist immigration law violators. IDENT did not include entry information.



access CCD when they adjudicated the BFCA cases, and gained access to the system on October 6, 2006.

Information found in the DOS's CCD and in the applicant's DS-156 Non-Immigrant Visa Applications may help identify fraud indicators that warrant further research. For example, in two of the proven fraud cases, information in the visa application or CCD record yielded indicators of possible fraud and prompted the FDNS IO to request overseas verification of documents.

In one case that was adjudicated prior to October 2006 when AOs gained access to CCD, a record in the DOS's CCD yielded sufficient evidence to substantiate a proven fraud finding. The case involved an asylum applicant who claimed that the government was persecuting him for his work as a manager of an anti-government entertainment group and for his family's opposition activities. In contrast to his statements on his application, the CCD record indicated that the applicant is a close relative of a high ranking government official and that the applicant was employed as a translator with a company that serviced foreign embassies. This information is inconsistent with the applicant's testimony.

CCD's utility extends beyond its ability to substantiate fraud; it provides information that can corroborate a legitimate claim or flag issues in a case that indicate fraud. In one case, the BFCA yielded an initial finding of proven fraud, but the finding was later changed to a finding of no asylum fraud. The initial finding was based on inconsistencies between testimony presented during the asylum adjudication and information presented to DOS in connection with a visa application that was obtained through CCD. Although this case initially contained indicators of visa fraud, ultimately the applicant was able to address the inconsistencies through an interview and provide a credible explanation that resulted in a finding of no fraud.

***(ii) Commercial Data Broker Checks Confirmed Fraud in 4% (1/29) of the Proven Fraud Cases:***

Commercial Data Broker records (CDBs), including Choicepoint and LexisNexis, yield valuable information about the identity, residence, and time an individual has been in the United States. CDB checks are not currently mandatory identity/background checks and are only conducted when a suspicious indicator that is unique to the individual case or to a pattern of cases has already been identified.

CDBs helped to uncover inconsistent records that established proven fraud in one BFCA case. CDBs also helped to find information indicating possible fraud in another 6% of the sample cases. In the one proven fraud case, the applicant claimed on her asylum application and in her interview that she entered the United States without inspection in October 2004. The CDB record linked a variant of the applicant's name and her exact phone number and date of birth to an address history dating back to 2002, indicating that the applicant misrepresented her date and mode of entry into the United States to circumvent the one-year filing deadline. This case was adjudicated by an office where all

AOs did not have access to CDBs. The Asylum Program has promoted increased access to and usage of CDBs by both AOs and IOs in asylum adjudications.

***(iii) Canadian Immigration Systems Checks Confirmed Fraud in 10% (3/29) of the Proven Fraud Cases:***

Asylum-related information that Canada shares with the U.S may affect case determinations. In this BFCAs, study information provided by the Canadian systems was sufficient to prove fraud in three cases. In one instance, an applicant entered the United States and filed an asylum claim based on sexual orientation. Canadian immigration systems checks revealed that the applicant previously claimed asylum in Canada based on persecution for political opinion and was denied. Because the information from Canada was gathered prior to the completion of the case, USCIS found the applicant ineligible for asylum based on the information that Canada supplied and referred the case to the immigration judge.

In another BFCAs case, Canadian immigration records revealed that the applicant previously applied for asylum in Canada. Although the AO had information that the individual had traveled in Canada previously and had relatives residing there, he or she did not have the information regarding the applicant's claim in Canada. Following up on the results of the biometric check yielded the inconsistent information that led to a finding of proven fraud.

***(iv) Overseas Document Verification Confirmed Fraud in 59% (17/29) of the Proven Fraud Cases:***

While asylum applicants are not required to submit documentary evidence, many individuals submit travel and/or other civil documents to help establish their identity and to support certain aspects of their asylum claim. In this BFCAs, most applicants provided documents at their asylum interview. Those documents included identity documents, political party membership cards, birth certificates, and hospital records.

The following are descriptions of the types of documents asylum applicants generally submit to support their claims:

- Law Enforcement Documents (arrest reports, imprisonment reports and any documents purported to have been issued by a government law enforcement entity);
- Medical Documents (medical reports and documents issued by medical establishments);
- Employment Documents (documents establishing an applicant's employment history);
- Political/ Religious Documents (documents issued by political and religious organizations that establish an applicant's affiliation with those organizations); and

- Identity/ Civil Documents (driver's licenses, marriage certificates, birth certificates or other documents issued by a civil authority to establish an applicant's identity and marital/family status).

Establishing asylum eligibility frequently involves determining if the documents submitted are authentic or fraudulent. Document fraud encompasses the counterfeiting, sale, and/or use of identity documents such as birth certificates, medical records, passports, and other documents used to obtain an immigration benefit. The knowing submission of a false document(s) as the foundation for a central element of an asylum claim may establish or serve as a factor to support an adverse credibility finding. Such fraud may call into question the reliability of other evidence submitted.

In many cases where documents were suspected to be fraudulent, the AO or IO submitted an overseas verification request. This process involves submitting the document to an overseas office of USCIS or DOS<sup>22</sup> to verify the authenticity of documents and/or other evidence submitted by an applicant. Depending on the information received, FDNS would include several document requests for the same case.

The BFCAs required that requests for overseas verification be limited because of the scarcity of United States government agency overseas positions and resources. Accordingly, FDNS IOs identified 59 (25%, or 59/239) BFCAs cases that were appropriate for submission of an overseas verification request. Twenty-six cases received overseas verification responses and 33 responses were not returned as of the issuance of this report. Of the documents submitted and responded to, 65% (17/26) were determined to be fraudulent. It is assumed that had more responses been received, more cases would be found to be proven fraud. Those documents that were discovered to be fraudulent as a result of overseas verification responses led to a proven fraud determination in at least 7% (17/239) of the BFCAs sample.

The BFCAs cases in which overseas verifications produced proven fraud findings illustrate how documents can be analyzed for fraud. In one case, the applicant was granted asylum based on past persecution and a well-founded fear of future persecution on account of her nationality<sup>23</sup> and due to ethnic discrimination in employment. Through overseas verification, USCIS determined that the applicant was employed with the same company for several years, and this employment contradicted the applicant's claims of work in another occupation. Overseas verification proved that her employment history was materially inconsistent with her asylum claim.

In another case, an applicant testified during his asylum interview that he was involved with a political opposition party. To support his claim, the applicant submitted two documents confirming his membership and activities in the party. FDNS IOs submitted

---

<sup>22</sup> For countries with USCIS presence, HQFDNS forwarded the document verification requests to USCIS HQ Office of International Operations. In countries with no USCIS presence, documents were forwarded to the Department of State, Bureau of Democracy, Human Rights, and Labor.

<sup>23</sup> In the context of the protected grounds contained in the refugee definition, "nationality" encompasses more than one's citizenship, referring also to the individual's ethnic origin and background.

these letters for overseas verification; both documents were found to be inconsistent with known exemplars, and ultimately proved fraudulent.

In a third case, the applicant was granted asylum based on past persecution and a well-founded fear of future persecution on account of her nationality. The applicant testified that, due to her ethnicity, she suffered severe discrimination in education and employment. USCIS discovered discrepancies regarding the applicant's educational level and employment history as listed on her visa application versus her asylum application, prompting an overseas verification request. Overseas verification consisted of an employment verification, and results confirmed that the applicant misrepresented her employment history in her asylum claim.

Another applicant testified that she suffered harm because of her political opinion. To corroborate her testimony, the applicant submitted a birth certificate and newspaper articles. FDNS IOs submitted these documents for overseas verification that resulted in a determination that they were fraudulent. In this case, the newspaper articles were found to be altered versions of original newspapers.

Thirty-eight documents that were sent for overseas verification were evaluated and responses were provided by the overseas post.<sup>24</sup> Of the documents that were verified, 66% (25/38) were determined to be fraudulent. 21% (8/38) of the returned documents were found to be genuine and 11% (4/38) of the documents were classified as suspected fraud.

See **Table 4** for a breakdown of the overseas verification responses by document type. This table does not illustrate the total number of cases for which overseas verification was requested and does not include the requests for which an overseas verification response was never received.

---

<sup>24</sup> Unverifiable documents include those that were sent overseas for verification, and the response received was that the document was unable to be conclusively verified as genuine or fraudulent.

**Table 4. Overseas Document Verification Responses by Type**

	<b>Confirmed Fraud Documents</b>	<b>Suspected Fraud</b>	<b>Genuine Document</b>	<b>Unverifiable Document<sup>25</sup></b>	<b>Type Submitted and Response Received (Total)</b>
Law Enforcement Documents	8	0	0	0	8 (21%)
Medical Documents	7	0	3	0	10 (26%)
Employment Documents	4	2	0	1	7 (19%)
Political/Religious Documents	4	1	2	0	7 (19%)
Identity/Civil Documents	2	1	3	0	6 (16%)
<b>Total # of Documents</b>	<b>25 (66%)</b>	<b>4 (11%)</b>	<b>8 (21%)</b>	<b>1 (3%)</b>	<b>38 (100%)</b>

Despite its utility, there were several disadvantages with the overseas verification process. First, a significant percentage of the submitted requests were never returned. At the time this report was written, requests for 56% (33/59) of the cases were still pending with the overseas office in which they were initiated. The inability and/or failure to respond timely to the requests have hampered FDNS IOs' ability to make timely and complete final fraud determinations on the 33 cases. Second, the response time is inconsistent and often lengthy. The average response time for overseas verification requests was 127 days with a range from five days to 342 days. 23% (6/26) of the cases where a response was received took over 300 days to complete. Another important limitation with this method is that overseas verifications must be conducted with particular care in asylum cases due to the confidentiality provisions contained in 8 C.F.R. §208.6. These provisions safeguard information that, if released to third parties, could endanger the security of the applicants or others who remain in the country of origin, or give rise to a plausible protection claim where one did not exist previously.

***(v) Admission of Fraud in the Course of ICE Investigation Confirmed Fraud in 4% (1/29) of the Proven Fraud Cases:***

Cases were not excluded from this study if they were subject to special handling or ongoing fraud investigations by ICE. In one case, the basis of the proven fraud finding was the applicant's admission of asylum fraud to ICE that was obtained in the course of an ICE investigation. Though this is not a specific fraud detection method applied to all cases in the BFCAs sample, this case demonstrates the valuable role that ICE can play in pursuing cases where fraud is suspected.

<sup>25</sup> Unverifiable documents include those that were sent overseas for verification, and the response received was that the document was unable to be conclusively verified as genuine or fraudulent.

### ***C. Analysis of the Data Revealed No Discernible Trends Across Several Variables***

The study population cases were analyzed to determine whether there was a relationship between identified proven fraud cases and the following independent variables: applicant's country of birth, gender, age, location of U.S. residence, port of entry, class of admission to the U.S., basis of asylum claim, time between when the applicant entered the U.S. and filed for asylum, interpreter used at the asylum interview, particular representative of the applicant, and the particular preparer of the asylum application, where not a representative. The assessment did not yield any discernable trends among the variables listed above when viewed on a nation-wide or sample-wide basis. The study population dispersed among all of the asylum offices and there was an insufficient number of cases from each office from which to draw any valid conclusions on individual office trends.

### ***6. Indicators of Possible Fraud Analysis<sup>26</sup>***

The majority of the cases in this study, 58% (138/239), were classified as exhibiting indicators of possible fraud as described below. Of these cases with indicators of possible fraud, 76% (105/138) were referred to an Immigration Judge independent of the BFCIA. Although these cases exhibited indicators of fraud that were material to asylum eligibility, such as inconsistencies between testimony and written statements, the indicators could not be confirmed by reliable evidence external to the applicant's testimony, which was a condition for classifying a case as proven fraud.

An asylum application may exhibit more than one indicator of possible fraud. A total of 153 indicators of possible fraud were identified in the sample and grouped into the five categories discussed below. The high rate of referral of these cases to the immigration judge indicates that current techniques and procedures that the Asylum Program utilizes in adjudicating cases are reasonably effective in dealing with cases that contain indicators of possible fraud.

#### ***A. AOs Referred to the Immigration Courts 54% (75/138) of the Cases Identified as Having Indicators of Possible Fraud Based on a Negative Credibility Determination.***

The credibility of an applicant's testimony is fundamental to establishing asylum eligibility. In many cases, it is the determining factor because the applicant's own testimony may be the only evidence provided to establish the facts on which the asylum claim is based. Asylum regulations require that adverse decisions include a separate assessment of the applicant's credibility (8 C.F.R. § 208.19). The credibility determination is part of the agency decision and cannot be arbitrary or capricious; therefore, the AO must explain his or her reasoning fully. The basic framework for determining credibility is found at INA section 208(b)(1)(B)(iii). This section identifies a

---

<sup>26</sup> In some instances, a case contained more than one indicator of possible fraud.

number of different factors, such as demeanor and candor among other characteristics that an AO can take into consideration as part of the credibility determination.

Typically, testimony that is specific, detailed, and consistent will be considered credible. Adverse credibility determinations are warranted if the applicant's testimony is found to lack detail, to be inconsistent, contradictory, or implausible. The written credibility determination must detail what type of deficiencies the adjudicating officer found and reflect that the applicant was given an opportunity to respond to the deficiencies. The credibility determination must also explain how these deficiencies are relevant to the adjudication. The submission of fraudulent documents that are represented as authentic and are used to prove an element material to the claim also warrants an adverse credibility determination.

AOs receive specific training and guidance on general considerations in evaluating the credibility of an asylum applicant, specifically the factors upon which a credibility determination may be based, the factors upon which a credibility finding may not be based, and how to determine whether any non-credible aspects of a claim affect eligibility.

A negative credibility finding, however, is not necessarily sufficient to support a finding of proven fraud. AOs denied or referred to the immigration courts based on a negative credibility determination in 54% (75/138) of the cases identified as having indicators of possible fraud. While insufficient persuasive evidence was submitted to convince the asylum officers that the alleged facts were true in these cases, no reliable external evidence could be found to confirm that the alleged facts were false.

***B. 10% (24/239) of Cases Contained a Pattern of Fraud Under Asylum Office/FDNS Monitoring.***

Of the sampled cases, 10% (24/239), are part of an identified fraud pattern that has been monitored by the Asylum Office or FDNS for newly uncovered patterns of possible fraud. These cases are not yet under ICE investigation. Examples of this category include a number of suspicious cases submitted by one immigration service provider or an unusual pattern of asylum claims.

BFCA cases were included in this category only where there was sufficient information to consider the applicant as fitting the pattern of interest. It was not sufficient to place a case in this category where the immigration service provider was subject to monitoring but where the applicant's claim or other significant case characteristics did not fit the suspicious pattern.

***C. 9% (22/239) of Cases Involved Individuals Under Investigation.***

In 9% (22/239) of the cases, applications were associated with an individual under investigation. The cases in this category were also associated with immigration service providers that were under investigation. The cases exhibited specific characteristics that were common among a group of cases with a particular immigration service provider.

Fraudulent providers can be a major element in all areas of asylum fraud; such providers include attorneys, preparers, interpreters, and notaries. These cases were referred by FDNS to ICE for further investigation and possible criminal prosecution.

#### ***D. Other***

In 3% (8/239) of the sample cases, indicators of fraud included material inconsistencies between testimony and/or supporting documentation, significant omissions from testimony and/or supporting documentation, or system checks produced information demonstrating suspected fraud.

### ***7. Actions Taken since the BFCA***

In the time since the BFCA cases were initially reviewed, the Asylum Program already has taken steps that further enhance the program's integrity, particularly with regard to increased systems checks against CCD and US-VISIT, as well as continued pursuit of additional information sharing agreements with other countries. The results of this BFCA validate the appropriateness of those additional procedural enhancements.

#### ***A. US Government Systems Checks:***

The Department of State's CCD aided in the detection of fraud in this BFCA. This system was not available to AOs at the time the BFCA cases were adjudicated. Since November 1, 2006, the Asylum Division has required officers to conduct a CCD check for any case in which US-VISIT (an automated, required check) indicates an existing visa encounter.

#### ***B. Information Sharing with Other Countries:***

The U.S. and Canada are authorized to share asylum-related information systematically and on a case-by-case basis with each other.<sup>27</sup> The Asylum Division now regularly exchanges information with Canada on individual asylum cases, when warranted, to confirm aspects of asylum eligibility. As part of the Asylum BFCA, biometrics of the BFCA principal applicants and their dependents were checked against Canadian immigration systems to determine whether the subjects had previously applied for refugee status in Canada. In cases where a search of these databases yielded a biometric match, the specific case information obtained was used to verify the credibility of the applicant's testimony in support of his or her U.S. asylum claim. In three instances in this study, Canadian records directly contradicted the asylum claim or conflicted with

---

<sup>27</sup> This exchange is authorized by *The Statement of Mutual Understanding (SMU) on Information Sharing between Citizenship and Immigration Canada, the U.S. Immigration and Naturalization Service, and the U.S. Department of State* (INF 4.1), along with its *Annex Regarding the Sharing of Information on Asylum and Refugee Status Claims*.



other information that the applicant provided the U.S government, thereby providing valuable information to the USCIS asylum application process.

The Asylum Division has completed information sharing pilot programs with the United Kingdom and Australia. The Asylum Division is expanding these efforts through its participation in the Biometrics and Technology Working Group of the Five Country Conference, and continues to explore the possibilities for information sharing with other countries in the future.

### **C. Overseas Document Verification:**

The Asylum BFCAs found that overseas verification of documents was the most instrumental tool in yielding evidence of substantiated fraud. That 29% (17/59) of cases sent for overseas verification resulted in a finding of proven fraud and 56% (33/59) of cases are still pending leads to the conclusion that USCIS could greatly benefit from an enhanced capability in this area as a component of a successful and effective asylum anti-fraud program. The Refugee, Asylum, and International Operations Division (RAIO) and FDNS have deployed FDNS personnel overseas. This will help USCIS complete more overseas document verification requests, and in a more expeditious manner. In April 2009, USCIS leadership published a memorandum providing interim guidance for overseas verification. Asylum verification requests must be redacted and channeled through FDNS IOs that track requests and route to appropriate offices for verification.

### **D. Additional Support for Investigation and Prosecution of Immigration Service Providers that Facilitate and Profit from Asylum Fraud**

This study revealed that of the 29 proven fraud cases, only one was under investigation by ICE at the time of the review. The role of ICE was critical in that case, as it was the admission of fraud made by the applicant to ICE that served as the basis for the proven fraud finding. However, among the cases found to exhibit suspected fraud, 22 were linked to an immigration service provider or pattern that was under investigation by ICE, while 24 cases were subject to asylum office monitoring due to characteristics that linked the cases to a suspicious pattern. As a general rule, a single indicator of fraud based on a suspicious pattern or link to a provider believed to facilitate fraud is not sufficient to support a denial or referral. In such cases, a successful fraud prevention program requires coordination with Law Enforcement Agency (LEA) partners to investigate and dissolve the fraud ring by identifying and prosecuting its operators.

Experience has shown that task forces that combine USCIS, ICE, DOJ, and other government agencies' resources in undertaking large-scale investigations can be highly successful in prosecuting asylum fraud facilitators and deterring fraud in the future. For example, Operation Jakarta, a federal investigation overseen by the United States Attorney's Office for the Eastern District of Virginia, uncovered several related asylum fraud rings and led to 26 criminal indictments of immigration service providers. This initiative was possible due to a committed fraud task force.

In May 2006 and April 2007, ICE Office of Investigations announced the creation of multi-agency Document and Benefit Fraud Task Forces (DBFTF) in cities across the nation including: Atlanta, Baltimore, Boston, Chicago, Dallas, Denver, Detroit, Los Angeles, Miami, New York, Newark, Philadelphia, Phoenix, San Francisco, St. Paul, Tampa, and Washington, D.C. DBFTFs have been created in many cities that contain Asylum Offices, and in 2008 eleven indictments were served for asylum fraud investigation cases through DBFTF efforts.

## ***8. Recommendations:***

As a result of information gleaned from this study, FDNS plans to issue internal agency recommendations to improve USCIS processes and fraud detection.

## ***9. Conclusion:***

Given the nature of the asylum eligibility requirements, the burden is on USCIS to employ as many tools as possible to verify that applicants qualify for the benefit and are not fraudulently representing themselves. FDNS examined various aspects of the Asylum Program and relevant fraud vulnerabilities during the Asylum BFCA. Although no discernible fraud patterns were detected as a part of this study, valuable information was obtained as to information gathered in the adjudications process that could inform the adjudicator about the possibility of fraud occurring as part of the filing.

The tools used here, systems checks and overseas document verifications, were useful in detecting fraud. Each method has relative advantages and disadvantages. Systems checks provide critical information about an asylum applicant, including date of entry in the United States, whether the applicant applied anywhere else, and what information the applicant provided the Department of State to obtain a visa to the U.S., to name a few examples. Systems checks, particularly checks of CDBs, can be expensive to first implement, but then have low costs per unit. In addition, AOs can easily conduct these queries as part of the adjudication process. Overseas document verifications also provide critical information about an asylum applicant that in some cases cannot be obtained elsewhere.

Finally, for future studies it would be useful to obtain larger samples of cases for each office that would allow a rigorous analysis of the common characteristics that fraudulent applicants may possess in a given jurisdiction. While this study did not have a large enough sample for that scrutiny, this information would be helpful, for the Asylum Program and FDNS to identify other potential vulnerabilities and adjudicators to be aware of fraud patterns in the applicant pool.

**APPENDIX**

DRAFT

**FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE**

**MEMORANDUM OF AGREEMENT  
BETWEEN USCIS AND ICE ON THE INVESTIGATION OF IMMIGRATION  
BENEFIT FRAUD**

1. **PARTIES.** The parties to this Memorandum of Agreement (MOA) are U.S. Immigration and Customs Enforcement (ICE) and U.S. Citizenship and Immigration Services (USCIS), two components of the Department of Homeland Security (DHS).
2. **AUTHORITY.** In section 2(I) of DHS Delegation Number 0150.1, Delegation to the Bureau of Citizenship and Immigration Services, and in section 2(I) of DHS Delegation Number 7030.2, Delegation of Authority to the Assistant Secretary for the Bureau of Immigration and Customs Enforcement, USCIS and ICE received concurrent authority to investigate fraud involving immigration benefits available under the Immigration and Nationality Act (INA). In their respective delegations, USCIS and ICE were further directed by the Secretary of Homeland Security to coordinate the concurrent responsibilities provided under these Delegations. This MOA is being undertaken to advance the coordination between USCIS and ICE, as authorized by these Delegations.
3. **PURPOSE.** The purpose of this MOA is to set forth terms by which ICE and USCIS will work together to combat immigration benefit fraud. This MOA is limited in scope to the specific responsibilities described herein.
4. **SUPERSESION.** This MOA supersedes the February 14, 2006 MOA of the same title.
5. **POINTS OF CONTACT (POCs).** The ICE POCs will be the Headquarters Identity and Benefit Fraud Unit (HQIBFU) and Public Safety and Human Rights Unit (PSHRU), the National Security Unit (NSU), the ICE Benefit Fraud Unit (BFU), Group Supervisors, and designated field IBF Units. The USCIS POCs will be the Headquarters Office of Fraud Detection and National Security (HQFDNS), Center Fraud Detection Units (FDU), and Field FDNS Operations.

**FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE**

6. RESPONSIBILITIES. The parties' responsibilities under this MOA are as follows:

A. USCIS

- 1) Each USCIS Office will designate an Office Director or Supervisory Immigration Officer (SIO) as point of contact to ensure cooperation, communication, and coordination with its designated ICE counterparts.
- 2) The primary USCIS component responsible for anti-fraud activities is the HQFDNS.
- 3) USCIS will pursue and continue its liaison activities with law enforcement and intelligence agencies in furtherance of vital information sharing, to include: conducting systems checks and comprehensive database runs or "sweeps", retrieving and reviewing hard copy files, and sharing subject matter expertise. FDNS will enter and track other agency unclassified information requests in its Fraud Detection and National Security Data System (FDNS-DS). USCIS components will perform de-confliction by querying principal SUBJECT names in The Enforcement Communication System (TECS) for inquiries relating to specific individuals. All TECS hits will generate a record of the transaction and provide an immediate notification to ICE. USCIS will ensure that employees using TECS who make these inquiries have accurate contact information in the system, so that ICE can respond appropriately to the notification. In addition, USCIS will notify the inquiring agent that a TECS record exists, but will not disclose the content of the record to any entity outside of DHS without the prior permission of the record owner. If a TECS record is not discovered during de-confliction, USCIS will nevertheless record the transaction and refer any DHS-external agency to ICE if the inquiry and apparent violations under investigation fall within the purview or authorities of ICE. Any disclosures will be in accordance with DHS policy and Federal law.
- 4) USCIS efforts will primarily focus on detecting and combating fraud associated with applications and petitions for immigration benefits. When USCIS refers a case to ICE for investigation, USCIS will suspend adjudication for 60 days. USCIS may resume its administrative process should ICE not respond to a request for investigation within 60 days, or provide a Case Closure Notice or case status report on an ongoing investigation within 120 days of accepting USCIS' request for investigation. USCIS will not suspend adjudication beyond 60 days absent a written request from ICE or approval of HQFDNS.
- 5) USCIS will refer articulated suspicions of fraud to ICE via the appropriate ICE Benefit Fraud Unit (ICE BFU) or other entity designated by ICE.

**FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE**

USCIS' primary vehicle in referring suspected fraud cases is FDNS Operations. USCIS will not refer individual applications or petitions involving suspected fraud to ICE unless (i) the alien is from a country designated in writing by ICE, (ii) the alien is the subject of a TECS II record, (iii) USCIS suspects misconduct on the part of the attorney, notary, interpreter or preparer; or (iv) evidence of a criminal conviction for an offense that is not grounds for inadmissibility or removability is present. Referral of single-issue fraud cases where an applicant has evidence of such a conviction will neither conflict with, nor supersede existing USCIS policies or established processes for egregious public safety criminal referrals.

- 6) USCIS Center FDU will refer suspect fraud cases to ICE BFUs through its tracking system. USCIS field offices may informally refer information to an ICE SAC office, so long as the referral is entered into USCIS' FDNS-DS or such other tracking system as FDNS may designate.
- 7) If ICE declines or rejects a USCIS referral, any further action taken by USCIS is considered administrative in nature. USCIS may conduct further inquiry when fraud is suspected, the primary objective of which is to pursue the information necessary to render a proper adjudication. Prior to making contact with the suspect entity, USCIS will de-conflict by querying subject records in TECS II. Should a TECS II record be found, USCIS will consult with the record owner regarding all TECS postings, pursuant to the contact instructions, to ensure its administrative inquiries will not negatively impact a criminal or national security investigation. If the administrative inquiry discloses criminal activity beyond what was initially suspected, USCIS will consult with ICE to determine whether ICE will open a criminal investigation
- 8) USCIS will support ICE in its criminal investigation of large-scale fraud schemes by conducting internal systems searches, providing subject matter expertise, and when necessary, court testimony.
- 9) USCIS will participate in the ICE-led interagency Document and Benefit Fraud Task Forces, as well as support local Joint Terrorism Task Forces.
- 10) A referral by USCIS to ICE does not constitute a withholding of adjudication under 8 C.F.R. § 103.2(b)(18) unless all the requirements of that regulation have been met. When a USCIS administrative inquiry results in a legally sustainable finding of fraud, it will deny the application or petition, and pursuant to the existing June 20, 2006, MOA between ICE and USCIS on the issuance of Notices to Appear (NTA), place the applicant or beneficiary in removal proceedings. Upon receipt of case closure notices where ICE has found fraud and identified subjects amenable to removal; USCIS will initiate removal proceedings through

**FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE**

issuance of NTA, pursuant to the existing June 20, 2006, MOA between ICE and USCIS on the issuance of notices to appear. FDNS shall be the primary POC for ICE regarding the disposition of referrals for administrative action.

- 11) USCIS FDUs will meet with their ICE BFU counterparts and Field FDNS Operations with their local ICE counterparts on a regular basis to address operational issues and maintain open lines of communication. Any and all issues that cannot be resolved, as well as issues that are national in scope, will be elevated to HQFDNS through the established chain of command. USCIS' HQFDNS will also meet with ICE's IBFU on a regular basis.
- 12) USCIS will conduct TECS checks on individual applicants, beneficiaries, and petitioners in accordance with relevant policy and guidance. USCIS will take the follow-up action specified in the record instructions. USCIS will contact the Terrorist Screening Center (TSC) on hits pertaining to known or suspected terrorists. USCIS will de-conflict cases containing national security-related concerns with the applicable local JTTF prior to rendering a final decision on an application or petition. HQFDNS will address issues of concern or national in scope with ICE's National Security Unit (NSU). HQFDNS will meet with NSU on a regular basis.
- 13) USCIS will continue to provide ICE access to appropriate systems to support anti-fraud efforts, as well as the pertinent training at mutually agreed upon times and locations at no expense to USCIS.
- 14) USCIS will not disclose to any other person outside of the Department of Homeland Security, who does not have the need to know that a case has been referred for investigation or is physically located with ICE's Office of Investigation, without first obtaining permission from ICE.
- 15) USCIS will make ICE case closure notices available to its personnel on a *need to know* basis.
- 16) USCIS will commit personnel to its FDNS Operation sufficient to support this MOA, provided such commitment is consistent with relevant statutes, regulations, DHS policy, and USCIS resources.

**B. ICE**

- 1) ICE Office of Investigations (OI) is responsible for detecting, deterring, and conducting criminal investigations of immigration benefit fraud.
- 2) The primary ICE component responsible for anti-fraud issues is the Identity and Benefit Fraud (IBF) program. The primary ICE component

**FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE**

responsible for national-security related issues is the National Security Unit. The primary ICE component responsible for human rights violator issues is the Human Rights Violator and War Crimes Unit.

- 3) Each ICE Special Agent-in-Charge (SAC) will designate an Assistant Special Agent-in-Charge (ASAC) to act as the primary POC for its local USCIS field office. The ASAC will designate a responsible party for regular communication and coordination with his or her USCIS counterparts.
- 4) ICE BFUs will conduct case reviews and refer cases amenable to criminal prosecution for fraud to the appropriate ICE OI SAC for investigation. Those cases not accepted will be returned to the referring USCIS FDNS unit. When referring cases to the field for criminal investigation, ICE BFUs will use the TECS II Case Management System. The BFUs will monitor case progress when accepted, per TECS-II reporting requirements.
- 5) When a suspected fraud case is referred to ICE BFU by USCIS, ICE BFU will decide whether to accept (open internally and assign to a SAC office) or decline (return to USCIS) the requested investigation within 60 days of receipt of the referral and notify USCIS immediately thereafter. Once the ICE BFU has accepted a case, it will refer the information to an ICE SAC office for investigation. Within 120 days of accepting a referral from USCIS, ICE will provide USCIS a case status update if it requires the continued suspension of adjudications. The report will include a determination of whether or not disclosure of information related to the investigation to the applicant or petitioner would adversely affect the ongoing investigation. If ICE does not notify USCIS in writing of the request for continued suspension within the 120 day timeframe, USCIS may resume adjudication at its discretion without further consultation with ICE. Similar updates shall be provided by ICE within one year after acceptance of the referral, and every twelve months thereafter. These time periods shall not limit in any way the length of time it may take for ICE to fully investigate a case.
- 6) Based upon the evidence available, local prosecutorial guidelines, and other relevant factors, ICE will determine whether to present the case to Federal, State, local, or tribal authorities for prosecution. The decision to criminally prosecute the case will ultimately lie with the prosecuting authority and remain subject to the standards of acceptance set by the prosecuting attorney.
- 7) Upon completion of each investigation, ICE will provide USCIS with a case closure notice containing the findings of the investigation; this includes information that can be provided to the alien or petitioner as part



**FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE**

of the decision on the application or petition without further authorization from ICE. ICE will place aliens convicted of fraud and other criminal charges as a result of ICE investigations into removal proceedings pursuant to the existing June 20, 2006, MOA between ICE and USCIS on the issuance of notices to appear.

- 8) ICE BFUs will meet with their USCIS FDU counterparts, and Field ICE SAC-designated agents will meet with their local USCIS FDNS counterparts on a regular basis to address operational issues and maintain open lines of communication. Issues that cannot be resolved, as well as issues national in scope, will be elevated to ICE's IBFU through the established chain of command. ICE's IBFU will also meet regularly with USCIS' HQFDNS.
- 9) ICE will commit sufficient personnel to the BFU program to support this MOA, provided such commitment is consistent with relevant statutes, regulations, DHS policy, and ICE resources.

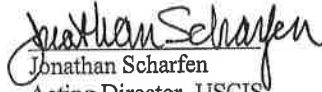
**7. DISCLOSURE AND USE OF INFORMATION**

- A. Any information disclosed under this MOA will be made pursuant to all relevant laws, regulations and policies including, but not limited to, the Freedom of Information Act, Privacy Act, and statutes limiting disclosure of information relating to immigration benefit requests for asylum and other forms of protection. Likewise, the handling of information shared as a result of this MOA within DHS shall be consistent with all DHS directives. ICE and USCIS understand that information exchanged or received pursuant to this MOA is not to be disclosed to other parties outside of DHS without first obtaining permission from the party that originated the information.
  - B. A request for information made under a court order, the Freedom of Information Act, Privacy Act, or via Congressional inquiry or the media that pertains to data obtained from the other agency requires the concurrence of that originating agency prior to the release of the information.
8. **OTHER PROVISIONS:** Nothing in this MOA is intended to conflict with existing laws, regulations, or DHS directives. If a term of this MOA is inconsistent with such authority, then that term shall be invalid. However, the remaining terms and conditions of the MOA shall remain in full force and effect.
  9. **EFFECTIVE DATE:** The terms of this MOA will become effective upon signature.


**FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE**

10. MODIFICATIONS: This MOA may be modified upon the mutual written consent of the parties.
11. TERMINATION: The terms of this MOA, and any subsequent modifications consented to by both parties, will remain in effect until modified or terminated. Either party can terminate this MOA by providing at least 60 days advance written notice to the other.

SIGNATORY AUTHORITIES:

  
Jonathan Scharfen  
Acting Director, USCIS  
Department of Homeland Security

9/25/08  
Date

  
Julie L. Myers  
Assistant Secretary, ICE  
Department of Homeland Security

9/11/08  
Date

Attachment

### **Grandfather Clause for Referrals Made Under Original MOA**

For any case referred to ICE by USCIS prior to the effective date of this MOA, ICE will confirm with USCIS in writing within six months of the effective date of the MOA whether the ICE BFU will retain the case for investigation and whether continued suspension of adjudications is required. If ICE determines that continued suspension is required, ICE will provide USCIS with a written report that will include a determination of whether or not disclosure of information related to the investigation to the applicant or petitioner would adversely affect the ongoing investigation. If ICE does not notify USCIS in writing of the request for continued suspension within the six month timeframe, USCIS may resume adjudication at its discretion without further consultation with ICE. Similar updates shall be provided by ICE within one year after the determination to retain the case and every twelve months thereafter. These time periods shall not limit in any way the length of time it may take for ICE to fully investigate a case.

|

DRAFT