

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

A Review of U.S. Citizenship and
Immigration Services' Alien Security
Checks



Office of Inspections and Special Reviews

OIG-06-06

November 2005

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our DHS oversight responsibility to promote economy, effectiveness, and efficiency within the department.

This report assesses the strengths and weaknesses of the use of security checks by U.S. Citizenship and Immigration Services when processing applications for immigration benefits. It is based on interviews with employees and officials, direct observations, and a review of applicable documents.

The recommendations have been developed to the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

Contents

Executive Summary	1
Background	2
Results of Review	5
Scope of security checks should be improved with biometrics and strategic planning.....	5
USCIS should continue to improve accuracy and timeliness of check completion	15
USCIS can administer security checks more efficiently.....	28
Recommendations	35
Management Comments and OIG Evaluation	36

Appendices

Appendix A: Purpose, Scope and Methodology	39
Appendix B: Management Response to Draft Report	40
Appendix C: Security Checks for USCIS Immigration Forms	43
Appendix D: Major Contributors to Report	46
Appendix E: Report Distribution.....	47

Abbreviations

BCS	Background Check System
BSS	Biometric Storage System
CBP	Customs and Border Protection
CIO	Chief Information Officer
DHS	Department of Homeland Security
DOJ	Department of Justice
EOIR	Executive Office for Immigration Review
FDNS	Office of Fraud Detection and National Security
FY	Fiscal Year
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IAFIS	Integrated Automated Fingerprint Identification System

Contents

IBIS	Interagency Border Inspection System
ICE	Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
INS	Immigration and Naturalization Service
ISRS	Image Storage and Retrieval System
IT	Information technology
NAILS	National Automated Immigration Lookout System II
OIG	Office of Inspector General
RAPS	Refugee Asylum and Parole System
SOP	Standard operating procedure
USCIS	United States Citizenship and Immigration Services
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

Figures

Figure 1:	USCIS Quality Assurance – Errors Found	17
Figure 2:	OIG Sampling Results – Total Errors Found	18
Figure 3:	OIG Sampling Results –Type of Errors Found	19
Figure 4:	Security Checks for USCIS Immigration Forms	43

Executive Summary

The staff of the National Commission on Terrorist Attacks upon the United States reported that the Immigration and Naturalization Service's "inability to adjudicate applications quickly or with adequate security checks made it easier for terrorists to wrongfully enter and remain in the United States throughout the 1990s."¹ The full Commission recommended:

The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system, including a single system for speeding qualified travelers. It should be integrated with the system that provides benefits to foreigners seeking to stay in the United States. Linking biometric passports to good data systems and decision making is a fundamental goal. No one can hide his or her debt by acquiring a credit card with a slightly different name. Yet today, a terrorist can defeat the link to electronic records by tossing away an old passport and slightly altering the name in the new one.²

The Immigration and Naturalization Service (INS), followed by U.S. Citizenship and Immigration Services (USCIS), made multiple changes over the past decade to improve the adequacy of security checks, detect applicants who pose risks to national security and public safety, deter benefits fraud, and ensure that benefits are granted only to eligible applicants.

As part of its ongoing responsibilities to evaluate the effectiveness of Department of Homeland Security (DHS) programs and activities, the Office of Inspector General (OIG) conducted a review of USCIS security check activities. Our review assessed whether USCIS (1) selected security checks of appropriate scope; (2) properly completed checks and concluded them with timely referrals and denials when appropriate; and (3) conducted the checks in an efficient manner. The scope and methodology of this review are discussed in Appendix A.

¹ *9/11 and Terrorist Travel*, staff report of the National Commission on Terrorist Attacks upon the United States, p. 99, August 21, 2004.

² *The 9/11 Commission Report*, National Commission on Terrorist Attacks upon the United States, p. 389, July 22, 2004.

USCIS has several significant changes planned and underway for the conduct of security checks. The Office of Fraud Detection and National Security (FDNS), created in May 2004, has begun to provide centralized support and policy guidance for security checks. In addition, USCIS has two automated systems in development—the Background Check System and Biometric Storage System—that could streamline how USCIS runs, documents, and monitors checks.

Security checks need continued management attention. First, USCIS' security checks are overly reliant on the integrity of names and documents that applicants submit; consequently, better use of biometric data is needed to verify applicants' identity. USCIS has not developed a measurable, risk-based plan to define how USCIS will improve the scope of security checks. Second, except for a small number of benefits, USCIS' management controls are not comprehensive enough to provide assurance that staff completes checks correctly. For a minority of cases, slow, inconclusive, or legally inapplicable security check results cause applications to stall, but USCIS is pursuing several solutions to conclude stalled cases. Finally, USCIS needs improved automation to eliminate paper-based, duplicative, and inefficient security check processes. Because USCIS' management of security checks is still somewhat decentralized, more coordination will be required to ensure efficient progress in implementing the changes USCIS envisions.

We are recommending that USCIS: 1) expand the use of biometric identification techniques; 2) establish a comprehensive, risk-based plan for the selection and completion of security checks; 3) set objectives for the conduct and completion of checks and organize management controls to ensure they are met; 4) implement the Background Check Analysis Unit, Background Check System, and Biometric Storage System; and 5) define accountability and timelines for implementing these changes.

Background

On January 24, 2003, USCIS was created as part of the Department of Homeland Security. Along with Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE), USCIS became responsible for providing services formerly provided by the Immigration and Naturalization Service. USCIS processes over 50 types of benefits for immigrants and non-immigrants, including citizenship, asylum, legal permanent residence, work

authorization, and extension of stay. In Fiscal Year (FY) 2004, USCIS completed approximately 7.3 million benefit applications and received 5.9 million more. Five large processing centers managed most applications, but others were processed in more than 33 district offices and sub-offices, eight asylum offices, and USCIS headquarters. USCIS' FY 2004 budget of \$1.8 billion was composed of \$236 million in appropriated funds and about \$1.6 billion in fee revenues.

USCIS' first of six strategic goals is to ensure the security and integrity of the immigration systems, noting that "a secure homeland depends on the integrity of our immigration system."³ During the benefit application process, USCIS conducts security checks in order to prevent ineligible applicants from obtaining benefits and to help law enforcement agencies identify people who pose risks to national security or public safety. Depending on the application submitted, USCIS conducts up to four different types of security checks:

- **Interagency Border Inspection System name checks (IBIS).** Managed by CBP, IBIS is a database of lookouts, wants, warrants, arrests, and convictions consolidated from over 20 agencies. A complete IBIS query also includes a concurrent check of selected files in the Federal Bureau of Investigation's (FBI) National Criminal Information Center. USCIS began conducting automated, name-based queries of IBIS for all USCIS applications in 2002. With an average of 3.7 names per application to check,⁴ USCIS conducted over 27 million IBIS checks in FY 2004.
- **FBI fingerprint check.** The FBI's Integrated Automated Fingerprint Identification System (IAFIS) matches criminal history records from federal, military, and most state apprehensions. USCIS collects and electronically submits applicants' fingerprints for selected benefits such as naturalization, permanent residence, and asylum. IAFIS has been in place since 1999; before that time, INS manually submitted fingerprint cards for criminal history records checks. USCIS submitted 1.9 million fingerprints at a cost of \$31.9 million in FY 2004.
- **FBI name check.** This partially automated, name-based check searches over 86 million files documenting people who are the main

³ *USCIS Strategic Plan: Securing America's Promise*, p. 6, 2005.

⁴ Additional names per application may include family members and aliases, such as married names.

subject or referenced in an FBI investigation. USCIS electronically submits applicant names to the FBI National Name Check Program for benefits such as naturalization, permanent residence, and asylum. The legacy INS queried the main files since 1985 but added reference files to security checks in 2002. USCIS submitted 1.5 million names at a cost of \$6.0 million in FY 2004.

- **Automated Biometric Identification System (IDENT).** Asylum offices have used this automated fingerprint identification system since 1998. Managed by US-VISIT, IDENT enables agencies to screen fingerprints against several different database repositories. USCIS enrolls aliens applying for asylum in the IDENT-Asylum database, screening them against previously enrolled asylum applicants, the immigration lookout database of criminal aliens, and the immigration recidivist database of repeat immigration offenders. Asylum offices completed approximately 146,000 applications receiving this three-part check in FY 2004.

Appendix C summarizes which checks selected forms receive. In addition, depending on the benefit, USCIS checks administrative systems to review applicants' prior immigration history, entry and exits into the United States, student records, and immigration court records. When checks result in confirmed derogatory information, USCIS has an established process for completing the cases with denials and referrals to fraud investigators, law enforcement, and the immigration courts.

USCIS' current structure for conducting security checks has undergone many changes during the past decade. Previous Government Accountability Office (GAO) and OIG reports criticized the INS for its failure to complete fingerprint checks, failure to review check results during adjudication, inadequate controls to deter impostor applicants, inadequate security check procedures and training, and an improper emphasis on productivity at the expense of accuracy in determining whether applicants were eligible for benefits.⁵ INS, and later USCIS, made multiple changes to the security check process to control the conduct and use of security checks. These include the

⁵ *Alien Fingerprint Requirements in the Immigration and Naturalization Service*, Department of Justice (DOJ) OIG Report Number I-93-13, February 1994; *INS Fingerprinting of Aliens: Efforts to Ensure Authenticity of Aliens' Fingerprints*, GAO-GGD-95-40, December 22, 1994; *INS Criminal Record Verification: Information on Process for Citizenship Applicants*, GAO-GGD-97-118R, June 4, 1997; *An Investigation of the Immigration and Naturalization Service's Citizenship USA Initiative*, DOJ OIG, July 2000; and *Immigration And Naturalization Service's Premium Processing Program*, DOJ OIG Report Number 03-14, February 2003.

creation of application support centers to collect applicant fingerprints and naturalization quality procedures to guide adjudicators. A more recent change is USCIS' May 2004 creation of the Office of Fraud Detection and National Security to provide centralized support and policy guidance for security checks and anti-fraud operations.

USCIS continues to operate under production pressures, decreasing a FY 2003 backlog of approximately 3.7 million applications to less than one million by June 30, 2005. USCIS publicly attributed part of the backlog accumulation to the 2002 addition of IBIS name checks for all applications. Without compromising security, USCIS plans to eliminate the backlog by the end of FY 2006.

Results of Review

Scope of security checks should be improved with biometrics and strategic planning

USCIS standards for verifying applicant identity are vulnerable to fraud, which lessens the reliability of security checks based on those identities. USCIS intends to increase use of biometric identification but has no defined plans to do so. However, key changes in screening policy integration and information technology (IT) systems design and access are outside USCIS control. In order to align the layers of immigrant screening, and ensure USCIS' access to immigrant and screening data sources, greater DHS coordination is needed.

USCIS needs to do more to verify applicants' identity

The security and integrity of USCIS' benefits process is overly reliant on the integrity of applicants to provide accurate information about their identity and history. The majority of USCIS security checks examine information that applicants provide: names, dates and places of birth, and other biographic information. Name-based checks are necessary to query records such as those in IBIS, but they are vulnerable to identity fraud and have several other weaknesses. USCIS supplements name-based checks with automated and manual biometric checks using IDENT, IAFIS, the Image Storage and Retrieval System (ISRS), and paper records. Biometric checks help to verify identity and improve the accuracy of security check results. However, less

than a quarter of USCIS' application workload is subject to fingerprint checks; and only two percent receive automated biometric checks that verify identity throughout the application process. USCIS is building a Biometric Storage System (BSS) that will support using fingerprints in identity verification. Other plans to expand biometric checks require definition.

Relevance and accuracy of name-based security checks

Name-based checks are the majority of USCIS' security check workload. They enable USCIS to review a wide variety of lookout and criminal history records. Depending on the benefit involved, USCIS must determine whether applicants meet adjudicative standards related to national security, criminal history, and even good moral character. Therefore, USCIS considers beneficial the broad, name-based checks of FBI investigative files and IBIS, which includes records from over 20 agencies. Checking one of IBIS's sources alone, such as the FBI's Terrorist Screening Database, would not provide USCIS with the broad range of information relevant to adjudication. USCIS screens all applicants against IBIS, about 7.3 million completed applications in FY 2004. Depending on the benefit, a portion of applicants also receives the FBI name check and name-based checks against administrative records such as the Student and Exchange Visitor Information System. These systems do not support queries based on fingerprints or other biometric information.

However, the name-based checks are only as accurate as the supporting biographic information used to conduct them. For several reasons, USCIS has little assurance that the supporting biographic information is accurate and matches the identity of the applicant. First, the information is self-reported by applicants, who have an incentive to falsify the information to obtain benefits if they are not otherwise eligible. Second, U.S. documents that support the self-reported information, such as birth certificates and driver's licenses, are easy to falsify⁶—and USCIS accepts documents from all other countries. Plus, in many cases, USCIS accepts photocopied documents, which are more easily altered than originals. Third, USCIS does not routinely verify identity with alternative means, such as contacting bureaus of vital statistics to confirm birth certificates or crosschecking addresses with national records. GAO reported that alien use of fraudulent documents and identity theft is “extensive,” and the staff of the National Commission on Terrorist Attacks

⁶ GAO reported that its staff “easily” created fictitious identities and obtained driver's licenses, birth certificates, and social security cards, using computer equipment “readily available to any purchaser.” *Security: Counterfeit Identification Raises Homeland Security Concerns*, GAO-04-133T, p. 1, October 1, 2003.

reported multiple instances of terrorists obtaining and using fraudulent identity documents.⁷

The effectiveness of name-based checks is further limited by how the checks are run. Because of the manual data entry involved in creating and searching the records, misspellings and typographical mistakes can skew results. When people change their names, such as after marriage, the search may miss criminal records associated with the old names. Transliterations of non-English and hyphenated spellings also complicate name-based searches. Finally, name-based checks create a processing burden to sort through hits that do not relate to the applicant searched, which occurs frequently with common names. After an analysis comparing name-based and fingerprint-based checks of criminal history records, the FBI reported, “The great weight of the evidence supports the FBI and the CJIS APB’s [Criminal Justice Information Services Advisory Policy Board] conclusion that a name check of criminal history record systems is a ‘rough’ process which produces many ‘false negatives’ (in which a criminal is not identified) and ‘false positives’ (in which an individual without a criminal record is identified as having a record).”⁸

Limited use of biometric checks

Biometric information—photographs, fingerprints, iris scans, and other identifiers—provides a more reliable means of verifying identity and querying screening databases because people’s biometrics are unique and more difficult to falsify. They limit identity fraud as well as reduce false positive and false negative screening results. USCIS collects photographs with many applications but does not have a system for automated, facial recognition screening. Most of the biometric checks USCIS conducts involve fingerprints, which USCIS collects for about a quarter of its applications. Fingerprints enable USCIS to screen applicants against existing FBI and DHS databases.

- **The Automated Biometric Identification System (IDENT).** About two percent of applications completed in FY 2004 were screened in IDENT. By comparing the stored biometric data with fingerprints and

⁷ *Identity Fraud: Prevalence and Links to Alien Illegal Activities*, GAO-02-830T, p. 1, June 25, 2002; *9/11 and Terrorist Travel*, staff report of the National Commission on Terrorist Attacks upon the United States, August 21, 2004.

⁸ House Judiciary Subcommittee on Crime Regarding H.R. 3410 and Name Check Efficacy, Hearing on Crime Regarding HR 3410 and Name Check Efficacy, May 18, 2000 (statement of David R. Loesch, Assistant Director in Charge, Criminal Justice Information Services Division, FBI).

photographs that applicants resubmit at several points during the application process, the Asylum Branch “locks” an applicant’s identity to a single set of biometric and biographic information. This helps the Asylum Branch to prevent impostors from interviewing or collecting asylum decisions, to identify applicants who apply under more than one name, and to find and consolidate multiple application files. Staff said that IDENT has been very useful in reducing duplicate filings since its implementation in 1998. In FY 2004, the Asylum Branch’s screening against three IDENT databases (asylum enrollees, immigration lookouts, and immigration recidivists) yielded 2,000 confirmed hits, mostly immigration recidivists.

On an exception basis, when other security checks reveal derogatory information and the applicant’s identity is in question, some district office staff screen a walk-in applicant’s fingerprints with IDENT equipment left over from the 2002-2003 National Security Entry/Exit Registration.⁹ However, this is an unofficial practice. District offices do not store and re-check fingerprints to “lock” applicant identity as asylum offices do.

- **FBI fingerprint check.** Through IAFIS, USCIS submits applicants’ fingerprints to the FBI for a biometric check against criminal history records from federal, military, and most state apprehensions. As the FBI reported, the fingerprint-based check is more accurate than a name-based check of these records. USCIS conducted 1.9 million fingerprint checks in FY 2004; we calculated that almost a quarter of that year’s completed applications included this check. Even though it is fingerprint-based, this check has limited ability to verify applicants’ identity because the FBI does not keep fingerprints to crosscheck them against USCIS’ previous submissions.¹⁰ USCIS’ fingerprint storage system is still in development.
- **Other biometric checks.** For some cases, USCIS staff performs visual comparisons of photographs, fingerprints, and signatures stored in paper application files and the automated ISRS to help verify an applicant’s identity. Manual review of biometric information occurs for about half of the application workload and before fingerprint

⁹ The INS deployed IDENT-ENFORCE (Enforcement Case Tracking System) equipment to district offices to collect fingerprints and register aliens from selected countries. CBP and ICE now administer this program.

¹⁰ USCIS checks are considered administrative. The FBI does not keep fingerprints on file unless they were checked for criminal purposes.

collection at application support centers. Manual checks are slower and more vulnerable to error than automated ones, and they are not readily accessible to all staff. Staff said that paper applications are rarely on hand for immigration information officers handling walk-in appointments, and even adjudicators are sometimes unable to obtain files stored in different offices. In addition, staff we interviewed in late 2004 was still seeking access to ISRS, which the 2003 *Security Matrix Project Recommendations Report* encouraged USCIS to expand.

The government is moving toward greater use of biometric screening. Homeland Security Presidential Directive (HSPD) 11, “Comprehensive Terrorist-Related Screening Procedures,” directed the Secretary of Homeland Security and an interagency working group to submit to the President a plan to improve terrorist-related screening that includes security features “that resist circumvention to the greatest extent possible” and that defines what identifiers to use in screening, including biometric ones. As of October 2004, the Department of State collects fingerprints and photographs from all visa applicants, about 7 million per year, to screen against IDENT. For applicants exempt from fingerprinting, such as children under 14, the Department of State conducts automated facial recognition screening, which along with the fingerprinting, serves to lock identity. Between October 2004 and March 2005, the system identified almost 5,000 mala fide applicants. The biometrics collected by the Department of State are linked with United States Visitor and Immigrant Status Indicator Technology (US-VISIT), which also uses IDENT technology, and screens applicants with biometric identifiers.

USCIS’ limited ability to verify and lock applicants’ identity poses several problems. Without automated biometric identification, establishing that the hit from a name-based check matches the identity of the applicant can be labor-intensive. For example, USCIS reported that one service center required an average of 5.4 additional database queries to verify an identity match for each positive IBIS name check. Delays in obtaining file biometric information to verify identity can interfere in acting on lookouts and warrants. An immigration information officer reported an instance when he could not obtain a file containing biometric information in time to verify a walk-in applicant’s identity so that he could act on a security hit’s warrant before the day’s appointments ended and the applicant departed. The ultimate problem caused by limited identity verification, however, is that USCIS may provide ineligible aliens with benefits. Staff said rescission or revocation of benefits is rare and has a high legal threshold. Furthermore, a benefit from USCIS

assists aliens in applying for other benefits—driver’s licenses, social security numbers, bank accounts, and in some states, gun licenses—enabling the alien to embed into society legally.

The ten-year business and information technology modernization plans that INS’s Immigration Services published in 2001 support increased use of biometrics, as does the USCIS Strategic Plan issued in 2005. USCIS has not developed a risk-based plan that outlines how, when, and for what benefits expansion should occur, or that assigns accountability, timelines, and milestones for plan implementation. Nevertheless, USCIS is expanding its biometric capacity on an ad hoc basis. In late 2004, USCIS added fingerprinting for temporary protected status holders re-registering for benefits. In spring 2005, USCIS awarded a contract to build, test, and implement BSS to store applicant fingerprints and photographs. Under development for several years, BSS will support FBI fingerprint checks and will potentially compare BSS biometrics with alien biometrics in US-VISIT collected by the Department of State and CBP.

Senior officials said that USCIS’ use of biometrics has been constrained by the capacity of application support centers to collect the data. Application support centers collected 1.9 million fingerprint submissions in FY 2004, while USCIS’ full application volume was about 5.9 million receipts. Staff said that most application support centers could process more applicants, but they are limited by an inefficient computerized scheduling system and labor. Staff estimates that consolidating the five-part scheduling system could increase capacity by more than a million appointments per year. Draft information technology architecture documents from the Chief Information Officer discuss improving the scheduling system. USCIS is adding 173 federal and contract staff to application support centers in FY 2005.

USCIS should develop a comprehensive, strategic plan for enhancing security checks

Since 2001, USCIS has made a number of changes to enhance the coverage of security checks for immigration benefits applicants. The changes USCIS has made to the content of security checks have been reactions to perceived gaps, a 2003 review, and separate office initiatives. There is no apparent effort to develop a strategic plan for selecting and conducting security checks. USCIS needs to develop such a plan, using risk assessment to prioritize efforts and allocate screening resources.

In response to incidents in 2001 and 2002 involving benefits granted to members of terrorist groups, staff added IBIS checks for all applications, greater use of entry-exit data, and FBI name check screening of reference files.¹¹ In 2003, USCIS subject matter experts reviewed the battery of administrative and security checks to identify additional check needs and redundancies.¹² The resulting report recommended retaining existing IBIS and FBI name checks, expanding biometric checks, and increasing adjudicators' access to databases for further, optional checking. USCIS implemented several of its recommendations, such as increasing the validity period of IBIS checks from 35 to 90 days.¹³ Some recommendations were not completed, and at the time of our review, no staff was monitoring their implementation. However, discrete initiatives from FDNS and other offices continue to refine the security check structure. For example, the Asylum Branch recently added FBI name checks of asylum applicants' aliases.

USCIS has not used more comprehensive program analysis to allocate screening resources and develop a plan for security checks. In essence, USCIS has not determined whether the resources used for certain checks might be used to greater effect with other checks. USCIS has limited program and performance information in order to make such a determination. For example, there is no statistically valid measurement of the prevalence of mala fide applicants in different application pools.¹⁴ In addition, USCIS has collected little measurement information on the effectiveness of different checks. USCIS' automated systems do not provide program management information that ties together security check results and adjudication outcomes. FDNS is beginning to develop both types of information. Through the Benefits Fraud Assessment, expected to be completed in 2005, FDNS has begun to measure the frequency of mala fide applicants for six benefits that staff considers historically prone to fraud or high-risk.¹⁵ Also in 2005, FDNS began manually to collect information on adjudication outcomes associated with a sample of positive FBI name checks.

¹¹ *The Immigration and Naturalization Service's Contacts with Two September 11 Terrorists: A Review of the INS's Admissions of Mohamed Atta and Marwan Alshehhi, its Processing of their Change of Status Applications, and its Efforts to Track Foreign Students in the United States*, DOJ OIG, May 20, 2002; *Review of the Circumstances Surrounding the Naturalization of an Alien Known to be an Associate of a Terrorist Organization*, INS Office of Internal Audit, December 13, 2002.

¹² USCIS, "Security Matrix Project Recommendations Report," May 2003.

¹³ Increasing the validity period reduced the number of IBIS checks USCIS conducts.

¹⁴ *Immigration Benefit Fraud: Focused Approach is Needed to Address Problems*, GAO-02-66, January 31, 2002.

¹⁵ USCIS processes over 50 types of benefits.

Changes to the security check structure should be guided by these kinds of analyses and a comprehensive, prioritized plan that assigns accountability and timelines for implementation. For example, although USCIS has intended to expand biometric identification since at least 2001, it has not determined when and for which forms biometric checks should be added, and it is not clear who is responsible for the determination. To improve its ad hoc arrangement for enhancing security checks, USCIS should 1) assess the risks posed by different applicant types and the effectiveness of checks in addressing that risk; 2) select improvements that maximize the benefit to the integrity of the immigration system while managing cost; and 3) plan for any improvements by assigning accountability and timelines, in order to ensure aggressive progress and results in meeting objectives.

Need for Increased DHS Role

The comprehensiveness of any USCIS plan will be limited by its dependence on systems and policies developed outside of USCIS. In order to align the layers of immigrant screening, and ensure USCIS' access to immigrant and screening data sources, greater DHS coordination is needed.

The plans and policies of US-VISIT, CBP, and ICE shape the checks USCIS conducts:

- The US-VISIT systems architecture houses the biometric data that USCIS collects for asylum applicants and plans to collect for other applicants. US-VISIT has the potential to permit USCIS to screen IDENT-Asylum and BSS enrollees against US-VISIT records of visas, entries, and exits, in order to establish identity and travel history. This capacity is not yet established, but US-VISIT staff began in 2005 to discuss plans to link these databases.
- CBP manages the IBIS lookout system on which USCIS depends for the majority of its security checks. Currently, CBP sets the user profile that determines which IBIS records USCIS views. In December 2004, CBP folded into IBIS the National Automated Immigration Lookout System II (NAILS), which was USCIS' primary tool for managing lookouts and fraud alerts. CBP did not fully retain NAILS features during the consolidation, reducing USCIS' ability to adjust lookout records with information such as changes of immigration status that may resolve lookouts.

-
- ICE sets the policy for security checks for aliens seeking benefits through Department of Justice's (DOJ) Executive Office for Immigration Review (EOIR). USCIS staff conducts these security checks and provides documentation of status when the immigration court grants benefits. Previously, ICE had no standardized requirements for checking aliens applying for benefits through the courts, and USCIS completed checks according to its own standards before issuing documentation. Delays in completing USCIS security checks for court grantees exposed USCIS to several lawsuits. Starting in April 2005, ICE standardized a process that requires the completion of IBIS and FBI fingerprint checks and the initiation of FBI name checks. With limited exceptions, USCIS will no longer withhold documentation of status from court grantees until checks are complete according to USCIS standards.

DHS could do more to coordinate screening between its components. For example, USCIS and ICE disagree about the cost-benefit of holding a case until the FBI finalizes a pending response to name check hits, which takes over six months for one percent of cases. For example, ICE security check procedures allow an applicant to receive asylum while the FBI name check is still pending, which means the FBI believes it has investigative records on the applicant but has not completed collecting and reviewing them for transmittal to ICE. In contrast, USCIS holds asylum applications until the FBI name check is complete. Also, USCIS refused to provide documentation of status to ICE-processed asylees until they passed an FBI name check, which USCIS initiated for them. DHS headquarters and the Directorate of Border and Transportation Security did not resolve the disagreement between USCIS and ICE about whether waiting for completed FBI name checks has benefits outweighing its costs. After discussions, USCIS agreed to continue to initiate FBI name checks for its own and for ICE-processed applicants, but neither agency will wait for ICE-processed applicants to pass the FBI name checks before the case decision and documentation of status. Thus, screening procedures for the same benefits are inconsistent. DHS should reconcile the inconsistent interpretations of the check's cost-benefits to improve security and efficiency.

In coordinating screening, DHS may further assist USCIS by facilitating information sharing, not only within DHS but also with the FBI and other external agencies. The Memorandum of Understanding by which USCIS accesses IBIS is a 1993 document between the INS and U.S. Customs. It should be updated to clarify USCIS and CBP responsibilities for information

sharing. The memorandum specifies that INS must have separate agreements with the other users of IBIS in order to view their lookout records, which raises the question of whether USCIS must recreate agreements since the 2003 division of INS, or whether other agreements within DHS provide USCIS with lookout access. In another example, for several years USCIS asked the FBI to remove restrictions on USCIS' name-based queries of the National Crime Information Center. Citing the Privacy Compact of 1988, the FBI permits USCIS to submit fingerprint-based queries via IAFIS but restricts name-based ones.¹⁶ USCIS argues that name-based queries provide information more rapidly and efficiently. GAO recently reported that the Department of State visa adjudication process would be more efficient with greater access to these name-based queries.¹⁷ USCIS has been working with the Department of State to gain access.

DHS should facilitate USCIS' access to screening information and assist in the coordination of screening strategies among DHS components. Moving toward greater coordination of screening efforts, DHS recently established a Screening Integration Working Group, including USCIS and other DHS components, to plan a coordinated strategy for screening individuals. This fits the intent of HSPD-11 to emplace "a coordinated and comprehensive approach" to screening across immigration, law enforcement, intelligence, and security components throughout the government. As DHS expands its efforts to coordinate screening, USCIS screening should receive greater attention and support. Aliens are eligible for some USCIS benefits, such as interim employment authorization documents, even when security checks return derogatory results. Furthermore, USCIS serves as the sole screener of some immigrants who enter without inspection or visas, thereby avoiding screening by CBP and the Department of State. Benefits for which unscreened immigrants apply to USCIS include asylum, adjustment of status under INA § 245(i), temporary protected status, and potentially, proposed guest worker programs. The USCIS benefits process is the government's first opportunity to screen these aliens against intelligence and lookout records.

¹⁶ These fingerprint- and name-based queries of the National Crime Information Center review federal and state criminal history records (charges and convictions) in the Interstate Identification Index. Currently, USCIS uses name-based queries of the National Crime Information Center only when other screening indicates the applicant has a criminal history. The FBI name check discussed elsewhere in this report, which is conducted through the National Name Check Program, reviews records of previous and ongoing FBI investigations.

¹⁷ *Strengthened Visa Process Would Benefit from Improvements in Staffing and Information Sharing*, GAO-05-859, September 13, 2005.

USCIS should continue to improve accuracy and timeliness of check completion

USCIS quality assurance and OIG sampling show that USCIS staff completes most required security checks. However, USCIS does not have comprehensive controls to prevent and identify mistakes when they occur. Further, USCIS has difficulty creating and retrieving historical records that show what checks were done when. Additionally, for a minority of cases, delayed and inconclusive security check results stall application processing for long periods. USCIS is strengthening its structure for processing security check hits and concluding cases that involve fraud or national security concerns with timely denials and law enforcement referrals.

Management controls to ensure check completion need improvement

Because of the manual effort and judgment involved in adjudicating immigration benefits, including security checks, the process is vulnerable to human error. Although USCIS staff performs most security checks in compliance with procedures, file sampling conducted during routine USCIS quality assurance and our inspection revealed security check errors for every form type reviewed. The errors vary in significance from incomplete file documentation to the approval of benefits without review of positive security check hits. They also vary in frequency, from less than one percent per sample, which meets USCIS' designated acceptable quality level, to over 95 percent for one form sampled. Though there are few reports of USCIS approving benefits for the mala fide, incomplete checks present a security vulnerability. Management controls to ensure check completion, including documentation and quality assurance reviews, are not comprehensive and should be improved.

In its March 2005 Backlog Elimination Plan report, for the fourth quarter of FY 2004, USCIS indicated that application processing errors are controlled:

For cases reviewed during the fourth quarter of 2004, USCIS achieved an overall processing accuracy rate of 99.6% and a critical processing accuracy rate of 99.7%, exceeding the minimum acceptable accuracy rates of 96% and 99% respectively. In all cases, corrective actions to prevent future problems were implemented. It was also verified that in applications where errors were detected, no applicant received a benefit for which he/she was not eligible.

“Critical” errors, which may occur in no more than one percent of forms reviewed in order to meet the acceptable quality level, include errors in security checks. In fact, security check errors are the most common critical error found during national quality assurance reviews. For the quarter described, the 80 critical processing errors involved IBIS name checks (72 instances) and FBI fingerprint checks (three instances). Critical errors found in the remainder of FY 2004 are in similar proportion. USCIS’ fourth quarter FY 2004 quality assurance report added, “Although, the Service is experiencing a trend in IBIS errors (a trend indicates that there is a system, process or procedural problem that needs to be addressed), the errors are within the Acceptable Quality Levels.” The trend continued in the first quarter of FY 2005, and USCIS reported it was studying IBIS name checks and anticipating improvements in procedures and training.¹⁸

However, these reports do not reflect all USCIS application processing. The national quality assurance program discussed above involves only the N-400 *Application for Naturalization*, which was 8.7 percent of USCIS’ completed applications in FY 2004. Because the N-400 is completed with different automated systems and standard operating procedures (SOPs), its quality results are not indicative of other forms’. In February 2005, USCIS added national quality assurance reviews for the I-485 *Application to Register Permanent Residence or to Adjust Status*, covering service center and district office processing. Additional monthly quality assurance reviews are conducted by Service Center Operations, which in FY 2004 reviewed the I-485, I-130 *Petition for Alien Relative*, and I-539 *Application to Extend/Change Nonimmigrant Status*. Service Center Operations suspended review of the I-539 in June 2004 and began reviewing the I-130 in August 2004. In sum, each month up to a third of USCIS’ completed applications is subject to random sampling for quality assurance.

Overall error rates are higher for the I-539, I-130, and I-485 than for the N-400. Furthermore, errors in the I-130 and I-485 samples exceed the one percent acceptable quality level for critical errors. Although USCIS does not monitor the proportion of security check errors as a whole, we extrapolated the following from monthly and quarterly reports:

¹⁸ “Quality Management Summary, Consolidated Service-Wide Quality Results – 1st Quarter FY 2005,” April 14, 2005.

Figure 1: USCIS Quality Assurance – Errors Found

Form	Months reviewed	Files reviewed	Files with errors	Proportion of files with errors	Files with security check errors¹⁹	Proportion of files with security check errors
I-130 <i>Petition for Alien Relative</i>	8/04-9/04	2,707	177	6.5%	44	1.6%
I-485 <i>Application to Register Permanent Residence or to Adjust Status</i>	10/03-9/04	9,521	539	5.7%	190	2.0%
N-400 <i>Application for Naturalization</i>	7/04-9/04 ²⁰	10,246	272	2.7%	75	0.7%
I-539 <i>Application to Extend/Change Nonimmigrant Status</i>	10/03-6/04	12,399	533	4.3%	70	0.6%

To extend our assessment of the risk of security check errors among USCIS applications, we sampled eight of the remaining forms that do not receive quality assurance reviews from USCIS. The eight forms represent an additional 51.3 percent of USCIS' FY 2004 workload and require different combinations of IBIS name checks, FBI fingerprint checks, and FBI name checks. We narrowed our sample to FY 2004 approvals in order to identify whether applicants received benefits despite incomplete checks. For further description of the sampling methodology, see Appendix A.

Every form type in our sample showed files with undocumented, untimely, or missing security checks. For the N-400, USCIS guidelines consider all these error types, including incomplete file documentation, to be critical errors. Although our sample and the quality assurance samples are not strictly comparable because of their different methodology, we note that the same types of errors occurred in higher proportion in every form in our sample, than in the forms receiving routine quality assurance reviews.

¹⁹ Individual errors noted on the reports included missing, untimely, unresolved, or undocumented IBIS name checks, FBI fingerprint checks, and FBI name checks. Untimely checks are ones processed after adjudication or more than 90 days prior for IBIS, or 15 months prior for FBI fingerprint checks. Unresolved checks are ones with hits confirmed on the applicant but not explained in the required resolution memorandum. The I-539 and I-130 receive only IBIS name checks.

²⁰ National quality assurance for the N-400 included all months of FY 2004, but until the fourth quarter, staff reported results by review item rather than by application file.

Figure 2: OIG Sampling Results – Total Errors Found

Form	FY 2004 approvals	Files reviewed	Files with security check errors	Proportion of reviewed files with security check errors
I-765 <i>Application for Employment Authorization</i>	1,213,534	112	10	8.9%
I-90 <i>Application to Replace Permanent Resident Card</i>	1,016,146	100	15	15.0%
I-129 <i>Petition for A Nonimmigrant Worker</i>	486,051	116	11	9.5%
I-821 <i>Application for Temporary Protected Status</i>	66,356	66	8	12.1%
I-881 <i>NACARA–Suspension of Deportation or Application for Special Rule Cancellation of Removal</i>	31,106	69	3	4.3%
I-730 <i>Refugee/Asylee Relative Petition</i>	24,492	47	30	63.8%
I-589 <i>Application for Asylum</i>	14,331	69	2	2.9%
I-192 <i>Application for Advance Permission to Enter as Nonimmigrant</i>	84	52	50	96.2%

In a follow-up to the sample, USCIS was able to demonstrate with automated and other records that many of the checks that appeared to be missing were in fact conducted but not documented in the file. Four form types showed errors solely in documentation and did not appear to be missing security checks.

The following table reflects the common error types we observed:

Figure 3: OIG Sampling Results –Type of Errors Found

Form	Total files with security check errors	Files with improperly documented checks	Files with missing, untimely, or unresolved security checks	Error type for missing, untimely, or unresolved security checks				
				IBIS Name check		FBI Fingerprint check		FBI Name check
				Missing	Untimely	Missing	Untimely	Missing
I-765	10	10	0	0	0	NA	NA	NA
I-90	15	15	0	0	0	NA	NA	NA
I-129	11	10	1	0	1	NA	NA	NA
I-821	8	4	4	1	1	1	1	NA
I-881	3	3	0	0	0	0	0	0
I-730	30	16	14 ²¹	6	8	NA	NA	NA
I-589	2	2	0	0	0	0	0	0
I-192	50 ²²	0	50	0	0	0	3	49

In particular, the I-192, I-730, and I-821 show substantial errors in processing security checks. For the IBIS check to appear missing in both the paper file and the automated case history, as seven I-730 and I-821 forms show, indicates that an automated IBIS check resulted in a positive hit, but the adjudicator did not review or resolve it before approving the case.²³ The other major error our sampling shows is a lapse in following the guidelines to conduct FBI name checks for I-192 forms. Of 52 files, 49 (94.2 percent) lacked FBI name checks. Staff at Vermont Service Center, which processed most of the I-192s in our sample, questioned whether the FBI name check is required for the I-192. But Chapter 42 of the *Adjudicators Field Manual* and several headquarters documents require the FBI name check and fingerprint check for the I-192.

Management controls to ensure check completion are inadequate

One explanation for the number of security check errors is that USCIS has not implemented sufficient management controls to limit errors. The low

²¹ USCIS claims that 13 of the missing or untimely I-730 IBIS checks may be solely documentation errors. The USCIS paper and automated records show no current check, but original forms were forwarded to Department of State for visa processing. For nine other original I-730 forms returned to USCIS, eight showed current IBIS checks and one did not.

²² Because some files contained more than one error type, the number of files with errors is not a sum of errors found.

²³ All of the forms in our sample, which excluded forms processed manually at the district offices, receive automated IBIS checks for the primary name that is data-entered. According to the processing rules, the Interim IBIS program updates the CLAIMS 3 automated case history when the IBIS check results in no hit. If a check results in a hit, CLAIMS 3 history will show no record of it; therefore, a history that is blank regarding IBIS checks implies an IBIS hit.

proportion of errors now shown on N-400s is achieved by several means,²⁴ including:

- Detailed, form-specific standard operating and quality review procedures;
- An automated processing system (CLAIMS 4) that prohibits adjudicators from approving cases until certain security checks are complete;
- Monthly quality assurance reviews, including correction of errors discovered and analysis of error trends; and
- Recurrent training for staff on processing standards and changes.

But the management controls for other forms vary, and in some cases, they are far less comprehensive. We identified several types of controls that USCIS could use more fully to limit errors. We acknowledge that varying levels of control can reflect management judgment about the risk involved in granting a specific benefit to a mala fide or unqualified alien and the costs of implementing stricter controls. Not all of the following controls are high-cost, however.

First, USCIS needs to improve how it documents and disseminates the policies and procedures for security checks. Communication of procedures is a longstanding issue for immigration services; in 1997 and 2001, GAO reported, “[P]oor communication was a problem, especially between headquarters and field units. For example, field and policy manuals were out of date and there was not one place that program staff could go for direction.”²⁵

No SOP summarizes the current security check requirements for all forms. Revisions to the outdated Chapter 16 of the *Adjudicators Field Manual*, “Fingerprinting and Other Agency Background Checks,” have been in draft for months. USCIS plans but has not begun to update the November 2002 SOP for IBIS name checks. In addition, although district office staff has had difficulty submitting and retrieving FBI name checks, they have no manual clarifying those procedures. In some cases, form-specific national SOPs consolidate security check guidance. Eight of the 12 forms discussed here

²⁴ In tandem with a critical report in 2000 from the DOJ OIG, USCIS (then part of the Immigration and Naturalization Service) reengineered the processing of the N-400 to limit errors. (*An Investigation of the Immigration and Naturalization Service’s Citizenship USA Initiative*, July 31, 2000).

²⁵ *Immigration and Naturalization Service: Overview of Recurring Management Challenges*, GAO-02-168T, p. 5, October 17, 2001; *INS Management: Follow-up on Selected Problems*, GAO/GGD-97-132, July 22, 1997.

have SOPs. The four that do not—the I-129, I-192, I-730, and I-821—were the ones that showed missing or untimely security checks. Most other forms do not have specific national SOPs either.

Additional security check requirements are reflected in a patchwork of memoranda and manuals. For example, USCIS issued at least seven memoranda altering security check procedures in March and April 2005. Staff at seven of 11 processing sites we visited expressed frustration with the quantity or insufficient clarity of changes to security check procedures. At three sites, staff maintains local guidelines to consolidate and clarify security check requirements.

Second, for some but not most forms, USCIS implemented automated controls on check completion. Naturalization forms processed in CLAIMS 4 and asylum forms processed in the Refugee Asylum and Parole System (RAPS) have automated, rule-based support that requires security checks to be complete before the adjudicator can approve the case. The Department of State has had similar controls in place for visa approvals since 1996. When checks result in positive hits, adjudicators must override them, which prevents overlooking hits.

Our sample included two forms processed in RAPS (the I-589 and I-881) and all security checks processed through RAPS were complete. However, USCIS processes the majority of forms in CLAIMS 3, which does not have these automated controls. All the forms in our sample with missing or untimely checks were processed in CLAIMS 3. Furthermore, some forms filed at the district offices are not supported by any of these national automated systems. USCIS staff reported that adding automated controls for forms processed in CLAIMS 3 or manually will be difficult until USCIS has a new automated case management system, planned since 2001 but not expected until 2007. However, even before fielding a new case management system, USCIS may better leverage automated controls on check completion. For example, automated controls ensured that IBIS checks were complete for the I-90s in our sample that were processed in CLAIMS 3 under Systems Qualified Adjudication rules.

Third, USCIS lacks a complete record of checks performed. USCIS needs the records to conduct quality assurance and supervisory reviews and to enable staff to refer to previous, current checks rather than duplicate them. When USCIS began IBIS name checks, guidelines required paper documentation of all checks: “The record will be updated to reflect the results of every IBIS

query ... When batch checks are conducted, confirmation that the check was performed must be placed in the file.”²⁶ The IBIS SOP supports full paper documentation. However, senior officials disputed whether all security checks must be documented in paper files, when automated systems also contain records of checks.

In our estimation, neither method currently provides adequate control because both are incomplete; and paper records in particular are vulnerable to error. Almost half of the security check errors discovered during our sampling (60 of 129, or 46.5 percent) involved paper documentation lapses. Some adjudicators continue to document IBIS checks by stamping applications. While quick, stamps in our sample were sometimes accompanied by illegible dates, results, and conductor initials, and stamps do not indicate which names were checked. The more detailed Record of IBIS Query, which the IBIS SOP requires, does record which names staff check. However, among over 300 forms in our sample where applicants listed more than one name, staff did not complete a Record of IBIS Query for 125. The paper records do not indicate whether staff performed IBIS checks on the aliases as required.

Automated records do not fully capture alias information, either. Furthermore, they do not reflect other important processing steps that are still performed manually: individual IBIS queries, adjudicator review of hits, and hit resolution. As a result, USCIS’ security check records are fragmentary. Incomplete records hinder staff in monitoring check completion and result in processing inefficiencies. Several managers and staff told us adjudicators routinely conduct new checks rather than rely on the file record. Additionally, incomplete automated records compel staff to conduct quality assurance manually.²⁷

Fourth, USCIS should reexamine its controls for reviewing check completion. USCIS has set national standards for formal quality assurance and supervisory review, but these reviews cover a small proportion of completed applications. As mentioned, national and Service Center Operations quality assurance samples up to a third of USCIS’ completed applications each month. National supervisory review of security checks occurs through the resolution memorandum for all IBIS name checks with confirmed hits, which are about two percent of IBIS checks. Additionally, supervisors in asylum offices use a checklist to review all security checks.

²⁶ “Interagency Border Inspection System Records Check,” July 2, 2002.

²⁷ USCIS does not have a process for auditing IBIS checks by reviewing the source records retained by CBP.

Beyond these reviews, processing offices provide a variety of supervisory and quality assurance checks. Four processing sites we visited, two of which were asylum offices, provided 100 percent supervisory review of security checks. Other offices review a percentage of applications completed, approved, or denied, sometimes based on form type or adjudicator tenure. Our concerns with this approach are twofold: 1) providing supervisory review based on form type can result in certain forms receiving no review; and 2) reviewing application denials is of lesser benefit to security because any mala fide benefit recipients are among the approvals. Quality assurance also varied among offices. Two processing sites we visited provided routine quality assurance for all forms; two, for all IBIS checks; and two were considering adding quality assurance for all IBIS checks. Other quality assurance staff with whom we met supplemented the national program with ad hoc reviews.

A number of forms are not subject to quality assurance. This is a missed opportunity for USCIS: staff reported that quality assurance reviews have helped to extinguish incorrect processing behaviors and provided a retraining opportunity. USCIS does not require refresher training on how to conduct security checks or procedural updates. An additional concern regarding quality assurance is that USCIS designated an acceptable quality level (for example, the one percent critical error rate) for only a few forms. USCIS should establish measures for the remaining forms or apply this one. It will be important for USCIS to continue to review security check performance and provide management with information to adjust management controls to ensure performance goals are met.

Incomplete security checks and weaknesses in USCIS management controls must be considered in context. Many USCIS applicants are bona fide. As GAO wrote in 1995, “While INS recognizes that even a relatively small number of aliens should not inappropriately receive benefits, it did not want to give the false impression that a criminal or terrorist receives a benefit every time a fingerprint check is not properly conducted.”²⁸ We agree that this holds true for any type of USCIS security check. For the files in our sample with missing or untimely IBIS checks, USCIS ran new queries and reported no derogatory information on all people checked. Three offices we visited reported similar experiences with correcting erroneous IBIS and FBI name checks. But whether USCIS’ incomplete security checks involve bona fide or

²⁸ *INS Fingerprinting of Aliens: Efforts to Ensure Authenticity of Aliens’ Fingerprints*, GAO/GGD 95-40, p. 4, December 22, 1994.

mala fide applicants is a matter of chance. In 2002, incomplete screening led a USCIS adjudicator to approve naturalization for a member of a terrorist group.²⁹ Though there are few reports of USCIS approving benefits for the mala fide, incomplete checks present a security vulnerability that USCIS should address through targeted improvements to management controls on check completion.

USCIS is implementing solutions to complete stalled cases

USCIS has an established structure for handling cases with security check hits and addressing national security, public safety, and fraud concerns. However, for a fraction of cases, slow, inconclusive, or legally inapplicable security check results can cause application processing to stall for months or even years. These delays can interfere with USCIS' concluding national security and public safety hits with timely denials or referrals to law enforcement. In addition, stalled cases decrease operational efficiency by reducing productivity and contributing to hundreds of lawsuits against USCIS. USCIS is pursuing several solutions to mitigate these effects and close stalled cases.

Staff described four primary ways that security checks could stall processing on a case:

- **Pending FBI name checks.** Unlike other USCIS checks that return results within a few days at most, the FBI name check takes more than a month to complete for six percent of submissions. For one percent, the FBI takes more than six months to compile the hit information and verify that the initial hit matches the identity of the applicant. In December 2002, USCIS (then INS) resubmitted 2.4 million applicant names for expanded checks,³⁰ almost double the number USCIS typically submits in a year's time. As of February 2005, USCIS reported 171,428 FBI name checks pending, including approximately 8,500 remaining from the December 2002 rerun. USCIS may pay the FBI double to "expedite" up to a few hundred FBI name checks per month. USCIS restricts these requests to certain cases, such as when the alien is about to become ineligible due to age, the applicant files writ of mandamus lawsuits to compel USCIS to complete adjudication,

²⁹ *Review of the Circumstances Surrounding the Naturalization of an Alien Known to be an Associate of a Terrorist Organization*, INS Office of Internal Audit, December 13, 2002.

³⁰ Ibid. In response to an incident that involved processing benefits for a member of a terrorist group, INS added searches of the FBI's reference file to searches of the main investigation file.

or other humanitarian factors. The “expedite” requests are insufficient to clear the backlog of FBI name checks.

- **Open cases referred to ICE for investigation.** When USCIS refers an open case to ICE for investigation, staff said long delays often occur before they receive clearance to complete the adjudication or another definitive response. In 2004, FDNS reviewed the IBIS national security/terrorism-related hit referral process and found that ICE was capable of resolving only about a quarter of the USCIS referrals in a timely manner. We observed rows of files USCIS staff shelved, pending a response from ICE. 8 C.F.R. § 103.2(b)(18) allows USCIS to place cases in formal abeyance and withhold adjudication when there is an ongoing investigation relating to the petitioner’s eligibility and disclosure to the petitioner would jeopardize the investigation.
- **Inconclusive results from checks and referrals.** Senior officials and staff said that security checks and supplementary information from FBI, ICE, or other record owners can sometimes be vague, inconclusive, or difficult to relate to the case adjudication. At one district office, staff said they shelved cases with complete, positive FBI name check responses for months, pending guidance on how to adjudicate them.
- **Legally inapplicable security check results.** In a 2003 audit, the DOJ OIG reported that INS could not deny the petition of an alien otherwise eligible for temporary worker benefits based on an IBIS hit.³¹ Unlike the adjudicative standards in the Immigration and Nationality Act for most benefits, the standards for adjudicating employment- and family-based petitions require USCIS to evaluate only the authenticity of the employment offer or family relationship, without regard to whether the person evokes security concerns. These employment- and family-based petitions serve simply to document the relationship, but they enable approved aliens to apply for other benefits such as legal permanent residence and visas from the Department of State. Nevertheless, USCIS would prefer not to approve any petition when security concerns have been identified. USCIS sometimes withholds adjudication through an informal

³¹ *Immigration and Naturalization Service’s Premium Processing Program*, DOJ OIG Report No. 03-14, February 2003.

abeyance; 8 C.F.R. § 103.2(b)(18) does not apply unless the investigation relates to the pending application.

Previous options that USCIS had for completing these four types of cases in a timely manner were insufficient. Given their partially automated systems, staffing level, and number of customers other than USCIS, the FBI's National Name Check Program officials said they could not complete USCIS' routine cases more quickly. The American Immigration Lawyers Association said that lawyers have begun to recognize that filing mandamus lawsuits helps to expedite FBI name check results. The USCIS Office of Chief Counsel estimated there were 1,000 cases filed in the federal courts last year naming USCIS as a party, of which 80 to 90 percent relate to security checks.³² This "solution" may assist applicants, but the volume of cases consumes USCIS time and resources that could be used elsewhere. Regardless, there are not enough "expedite" slots for all pending FBI name checks.

For the relationship-based petitions, USCIS options include withholding adjudication through an ongoing, informal abeyance; requesting that applicants withdraw the petitions; or approving the petitions in the expectation that applicants will be denied at another point in the process. However, delays from informal abeyance are also vulnerable to legal challenge. Furthermore, applicants can refuse to withdraw petitions, and the transfer of derogatory information to support later denial is not fail-safe. For some cases, USCIS relies on the Department of State to deny the alien a visa. USCIS forwards petitions stamped "admissibility concerns identified" to visa processing centers. Because information-sharing protocols prevent USCIS from revealing derogatory information it received from third parties, visa staff must attempt to recreate USCIS' hit. A Department of State manager said that they were not always able to do so.

Long-delayed cases increase USCIS' workload other ways, as well. IBIS and FBI fingerprint checks can expire, requiring new checks and repeated fingerprinting. In addition, adjudicators run queries on a regular basis for each case with a pending FBI name check, to learn whether FBI name checks cleared.

³² This figure is exclusive of litigation relating to the commercial and administrative law division.

Solutions USCIS is pursuing

USCIS has begun to address cases delayed with ICE and the FBI by assigning USCIS staff to work off the backlogs. In order to keep ICE's backlog from growing, FDNS ceased referring IBIS national security hits to ICE in November 2004, instead resolving them in house. In May 2005, FDNS assumed responsibility for the backlog of approximately 600 national security hit cases that had remained with ICE. In March 2005, USCIS detailed five personnel to the FBI National Name Check Program for up to a year to assist with the pending FBI name checks.

Additionally, USCIS has been pursuing regulatory and statutory options to expand authority to withhold adjudication and to deny benefits due to national security concerns. USCIS described the suggested statutory change as providing the legal basis "to deny any benefit to aliens described in any of the national security related provisions of inadmissibility or deportability in the Immigration and Nationality Act (INA), who are the subject of a pending investigation or case that is material to eligibility for a benefit, or for whom law enforcement checks have not been conducted and resolved."³³ However, USCIS has been pursuing similar changes for several years, and staff has no indication that their approval is imminent.

Meanwhile, USCIS is developing two specialist staff units to help conclude cases with complex adjudication and security check issues. In March 2005, USCIS created a unit called FOCUS within the Office of Field Operations to assist in the adjudication of selected cases with identified national security or public safety concerns. Both field offices and FDNS may refer cases to FOCUS for adjudication guidance. FOCUS's initial workload is 100 cases. USCIS has also proposed developing a Background Check Analysis Unit within FDNS to resolve the more complex and sensitive hits, receive and review all national security notifications to observe trends, provide direction and oversight to the field, and coordinate issues with other USCIS components including the Office of Chief Counsel. FDNS estimates the unit will resolve at least 500 complex and sensitive security checks per year. The reprogramming request to fund seven personnel to staff the unit was in the preliminary approval process as of April 2005.

³³ USCIS draft amendment adding a new Section 362 of the Immigration and Nationality Act, "Denial of Immigration Benefits to Terrorists and Criminals."

USCIS can administer security checks more efficiently

USCIS can strengthen the efficiency of its security check program. First, USCIS automation does not provide many of the efficiencies that existing IT solutions offer. USCIS needs improved automation to reduce duplicative, paper-based security check processes. USCIS has two systems in development that could streamline how USCIS runs, documents, and monitors checks. Second, more than a year after the creation of FDNS, many USCIS parties are still responsible for aspects of the security check program. While there are justifications for the diffused responsibility, clarifying accountability could better enable USCIS to address program weaknesses including the lack of an integrated, risk-based plan for which checks to conduct, lack of comprehensive program management data, and delays in disseminating uniform policies and standards.

Automated systems provide inadequate support for processing security checks

USCIS does not have a centralized, automated case management system or security checks system. A large portion of the security check process is completed and documented by hand or with homegrown systems. Compared to the Department of State's, USCIS' systems have limited ability to reduce duplication and processing steps, control approvals, document checks for audit purposes, and create adequate program management information. As a result, the process is labor-intensive, vulnerable to human error, and inefficient.

Several previous OIG and GAO reports have noted that USCIS does not have information systems adequate to support efficient processing of benefits and security checks.³⁴ Cases are not managed or tracked centrally: staff processes applications in CLAIMS 3, CLAIMS 4, RAPS, the Integrated Case Management System, the Marriage Fraud Amendment System, homegrown systems such as the Buffalo Examination Tracking System, and in some cases, no automated system. Furthermore, even cases that have automated records have paper records as well, which staff must create, track, update, and retrieve manually. Although staff initiates security checks electronically, they remain

³⁴ Audit Report: Fingerprint and Biographical Check Services Provided by the Federal Bureau of Investigation to the Immigration and Naturalization Service, DOJ OIG, Report No. 99-13, March 1999; Immigration Benefits: Several Factors Impede Timeliness of Application Processing, GAO-01-488, May 4, 2001; Immigration Benefit Fraud: Focused Approach is Needed to Address Problems, GAO-02-66, January 31, 2002.

largely a paper process. Staff and contractors review paper applications to find and screen applicants' aliases. Checks are documented and reviewed manually with IBIS stamps, handwritten Records of IBIS Query, Interim IBIS printouts, printed FBI Rap sheets, printed FBI name check results, and handwritten hit resolution documents.

The existing paper and automated systems have limited ability to:

- Prevent duplication of work. USCIS' automated systems do not store complete security check information in order to permit staff to review it electronically regardless of location. While national case management systems such as CLAIMS 3 and RAPS store security check dates and results, more detailed information such as hit content and resolution is available only in paper files and, in some cases, local systems. Therefore, when staff does not have the paper record to review—for example, an immigration information officer assisting a walk-in applicant—staff re-runs and resolves IBIS checks even if they are current. USCIS also does not have an automated system to store fingerprints. When fingerprints age past 15 months, which USCIS' backlog and slow FBI name checks can cause, applicants must return to application support centers to submit their fingerprints again.
- Automatically update screening results. The screening databases USCIS uses do not provide “wrap-back” updates that push updated records to USCIS when information on applicants whom USCIS has already screened changes. Instead, USCIS staff re-runs all IBIS name checks more than 90 days old before adjudication to see if any of the records have changed. Although USCIS studied and selected the 90-day expiration period to reduce the possibility of missing significant record updates, the potential exists. Like the IBIS check, USCIS repeats the FBI fingerprint check for updates on a 15-month expiration schedule. USCIS has not set an expiration period for the FBI name check, but the FBI considers a name check to be current for 120 days. However, updating FBI name checks also consumes labor as staff checks repeatedly whether pending name checks have finalized. Asylum Branch's IDENT checks are refreshed when applicants return to the asylum offices. Asylum staff has begun to receive some wrap-back information through US-VISIT, though headquarters staff must manually redirect it to local offices.

-
- Assist in verifying applicants' identity with biometric identifiers. Although USCIS collects fingerprints and photographs from many of its applicants, in most cases these are used for card production and criminal history record checks, not for automated, biometric verification of the applicant's identity. Visual inspection of biometric data to establish the applicant's identity is slower and less reliable than automated checks. Only the fingerprints that are stored in IDENT-Asylum are used for automated identity verification. However, this biometric check has limitations as well. US-VISIT does not crosscheck IDENT-Asylum files with its visa and entry-exit records, and asylum staff conducts manual, name-based searches of this information until US-VISIT improves cross-check capability.
 - Consolidate checks. The May 2003 *Security Matrix Project Recommendations Report* advised USCIS to develop “multiple system search capacity,” the ability to enter and review applicant information in a single system for checks conducted in several others. USCIS staff must log in to separate systems to initiate and review most IBIS, FBI, IDENT, and administrative checks. A March 2005 study indicated that derogatory information provided by FBI name checks was not consistently available via IBIS name checks, even though the IBIS check contains FBI information from the National Crime Information Center and Terrorist Screening Database. Therefore, for many applications, USCIS continues to run two security name checks, biometric checks, and administrative checks.
 - Generate national program management information. The systems USCIS uses do not track the resources used to process security checks, and none except RAPS tracks the check results. For example, national systems do not supply records of the number of IBIS checks conducted, the amount of time staff spends resolving hits, the number and types of IBIS hits received, and the adjudication results of cases with IBIS hits. USCIS has developed estimates of some figures based on data provided by individual service centers, which have more extensive automated support than district offices. Further information comes from ad hoc studies; other manually compiled reports; and the Performance Analysis System, the reliability of which DOJ OIG criticized.³⁵

³⁵ *Accuracy of Adjudications and Naturalization Data in the Performance Analysis System of the U.S. Immigration and Naturalization Service*, DOJ OIG Report No. 99-03, February 1999. In FY 2004, independent auditors reported internal

Improved automated systems that include these features would assist USCIS in eliminating duplication of work, increasing productivity, reducing opportunities for human error, and maintaining management controls. The Department of State developed systems that include some of these features. For example, an entry in the Department of State's Non-Immigrant Visa Processing System permits staff to initiate and review security check information in IDENT, the Consular Consolidated Database, Security Advisory Opinions, and the Consular Lookout and Support System. Consular officers can more quickly review the consolidated information, including historical records, without logging in and out to search different systems. The Non-Immigrant Visa Processing System also automatically checks applicant aliases, runs fingerprint and facial recognition biometric checks, and compares biographic data during checks to flag potential identity mismatches. Furthermore, the system incorporates management controls including rules that prevent approvals without security checks, complete historical records of security check information reviewed, and several means of reviewing case decisions.

Without these features, USCIS' security check processes are more labor intensive, vulnerable to human error, and difficult to monitor. For example, we estimated that refreshing IBIS checks to ensure they are current within 90 days at adjudication resulted in a minimum of 4.3 million additional IBIS checks in FY 2004. Conducting checks without automated controls on completion and renewal permits staff errors like those found during USCIS quality assurance and OIG sampling. And the lack of centralized, automated records for analysis causes USCIS to rely on less-definitive estimates and anecdotes for decisions. For example, USCIS has no record of how many relationship-based petitions staff was obliged to approve despite derogatory security check results. There is no estimate of the scale of the problem to help indicate whether the statutory change being pursued is the only viable solution.

USCIS has been planning to improve automated support for the security check process for several years. In December 2001, USCIS (then INS) issued an IT modernization plan³⁶ with goals to integrate the disparate case management systems; transition to a paperless system; and incorporate automated,

control weaknesses in USCIS' Performance Analysis System. (*U.S. Department of Homeland Security Performance and Accountability Report, Excerpts of Financial Information Part II, Seven Months Ended September 30, 2003*, KPMG LLP.)

³⁶ *Immigration Services IT Strategic Plan, 2002-2012*, December 2001.

biometric identification. USCIS does not expect to field a consolidated, automated case management system until 2007. However, other advances have been made. In 2004 and 2005, the National Benefits Center and lockbox application receipt operations began to enter data and pre-process applications for all district offices, partially automating this work, which includes initial name checks and fingerprint scheduling.

Furthermore, USCIS conceived two new software systems to support the background check process. The Background Check System (BCS), which USCIS began testing in spring 2005, will centralize check records, helping to reduce duplication of checks and supporting check reviews. Also in spring 2005, USCIS contracted to begin building the BSS, which will retain fingerprints, photographs, and signatures for screening. Once fielded, these systems should do much to reduce duplication and manual effort, and to improve USCIS' ability to monitor processing. USCIS' May 2005 strategic plan discusses integrating these systems with its case management systems and pursuing wrap-back updates from the agencies that supply check information.

USCIS has suffered delays in implementing its plans to modernize and automate its background check systems. Staff said that the BCS software were in development when Immigration Services split from the other offices of INS in March 2003. Under the DHS realignment, Immigration Services lost direct IT support, instead receiving it from ICE under a shared service agreement. USCIS recently reformed its IT infrastructure, integrating authority under the Chief Information Officer (CIO) in May 2005, and that office assisted in advancing BCS and BSS development.³⁷ USCIS succeeded in obtaining access to a test environment for testing BCS in spring 2005, and a contract to develop BSS followed. Continued progress will be necessary to eliminate obstacles to processing efficiency.

USCIS should continue reorganization of security check management

In previous sections, we discussed several improvements USCIS should pursue, including a risk-based plan to enhance the scope of security checks, more comprehensive program management information, and stronger management controls. FDNS has begun to provide some of this support for security checks. However, it shares responsibility for these areas with adjudicative and policy

³⁷ For further discussion of USCIS IT modernization and infrastructure, see *U.S. Citizenship and Immigration Services Is Not Effectively Managing Information Technology to Meet Mission Requirements*, DHS OIG (forthcoming).

offices including Service Center Operations, Field Operations, and the Office of Quality Assurance and Production Management. It also shares responsibility with the Asylum Branch and the CIO, which are outside the domestic operations organization where FDNS sits. Coordinating some of these parties has delayed at least one significant SOP change. In order to ensure aggressive progress in security check management, USCIS needs to establish accountability and timelines for developing security check plans, policies, and program information.

Announcing the official formation of FDNS in May 2004, the USCIS director defined its mission to:

- Oversee and enhance policies and procedures pertaining to the performance of law enforcement (background) checks on applicants and petitioners
- Identify and evaluate vulnerabilities in the various policies, practices, and procedures which threaten the integrity of the legal immigration process
- Recommend solutions and internal controls to address these vulnerabilities.³⁸

Since that time, FDNS reengineered procedures for resolving security check hits involving national security and developed new policies to support law enforcement and intelligence agencies interacting with benefit applicants. In February 2005, FDNS initiated its Benefits Fraud Assessment to statistically assess for the first time the percentage and type of fraud in six higher risk applications. The information from this study should enable FDNS to evaluate vulnerabilities, as will the information developed with FDNS's new automated Fraud Tracking System and planned Background Check Analysis Unit.

Several responsibilities related to policy, procedures, and controls for security checks are assigned outside FDNS. FDNS officials told us that the responsibility for planning the types of security checks to conduct belongs with the adjudicative offices such as the Asylum Branch, Service Center Operations, and Field Operations. Supporting this statement, the Asylum Branch and Service Center Operations initiated recent changes regarding how USCIS screens applicant aliases.

³⁸ “Introducing the Office of Fraud Detection and National Security (FDNS)”, May 2004.

For writing the policy defining user access to IBIS, or which type of records users at different security clearance levels can view, the Office of the CIO has responsibility. For the management control of quality assurance procedures and testing, the Office of Quality Assurance and Production Management, Service Center Operations, and selected field offices have been driving changes. Much of USCIS' quality assurance assesses performance other than security checks, but field offices are discussing plans to develop a quality assurance test solely for security checks. Offices other than FDNS also manage another control, security checks training. We observed several opportunities for making training more complete and uniform. Most field offices we visited lack recurrent training on changing security check policies and procedures, and staff requested more security checks training, such as on IBIS features.

In sum, security check administration is still somewhat decentralized within USCIS. While this is management's prerogative, we note that USCIS formed FDNS partially in response to a 2003 study that recommended USCIS centralize management of security checks. The centralization was intended to improve the efficiency and effectiveness of the security check process and eliminate "variability of background check requirements ... inconsistent administration of background check information ... [and] poor use of resources."³⁹

Although USCIS continues to refine its security check process, we did not observe efforts to unify the process under a plan with performance goals and measures, clearly defined accountability, and timelines for implementing changes. However, these steps are necessary to balance available resources, decentralized office responsibilities, and desired program outcomes. The Office of Management and Budget directs: "[R]esults-oriented managers must ask themselves if the programs they administer are achieving the desired result at an acceptable cost. If the answer is 'no' or 'we don't know,' they must do something about it, such as clearly define the desired outcomes, determine the causes of unsatisfactory performance, construct plans to remedy any problems, develop aggressive timeframes for taking action, and ensure that actions are implemented."⁴⁰

Without clear plans, accountability, and timelines, USCIS will have difficulty coordinating its offices to implement needed improvements on an aggressive

³⁹ *BCIS Background Checks: Identifying the Need for a centralized Background Check Unit (BCU)*, Booz Allen Hamilton, May 14, 2003.

⁴⁰ *The Federal Government is Results-Oriented: A Report to Federal Employees*, Office of Management and Budget, p. 1, August 2004.

schedule. For example, when our review began in October 2004, FDNS planned to revise the outdated 2002 SOP for IBIS. By the conclusion of our fieldwork in March 2005, FDNS and Service Center Operations had begun discussions on IBIS roles and responsibilities and potential SOP changes, to be followed by discussions with Field Operations and other IBIS users on an indefinite timeline. It is unclear when the revision will be complete, and as we noted on page 21, field offices have begun compiling local guidelines in the absence of a current IBIS SOP. The risk of this alternative is that local offices will develop guidelines that do not fully comply with the official SOP, which was the case at one office we visited.

Recommendations

We recommend that U.S. Citizenship and Immigration Services:

Recommendation 1: Expand the use of biometric identification in security checks, as consistent with risk assessment.

Recommendation 2: Establish a comprehensive, risk-based plan for the selection and completion of security checks.

Recommendation 3: Set measurable objectives for the conduct and completion of all security checks and reorganize management controls to ensure objectives are met.

Recommendation 4: Implement the Background Check Analysis Unit in the Office of Fraud Detection and National Security.

Recommendation 5: Implement an automated system that stores applicants' biometric information and supports its use in security checks.

Recommendation 6: Implement an automated system that supports running, documenting, reviewing, and monitoring security checks.

Recommendation 7: Define accountability and timelines for implementing changes to the security check process that include the development of the plan for completion of security checks, check completion objectives, and reorganized management controls.

Management Comments and OIG Evaluation

We evaluated USCIS' written comments and made changes to the report where deemed appropriate. Below is a summary of USCIS' written responses to our recommendations and our analysis of the response. A copy of USCIS' response in its entirety can be found in Appendix B.

USCIS agreed that its security check process requires improvements including consolidated management, clarified procedures, and increased monitoring. USCIS added that better automated tools, which are in development, are fundamental to process improvements. In addition, USCIS stated that it will continue to pursue access to automatic updates for changing security check information, i.e. wrap-back. We agree the wrap-back feature could play a vital role in improving both the security and efficiency of USCIS checks.

Recommendation 1: Expand the use of biometric identification in security checks, as consistent with risk assessment.

USCIS Response: USCIS acknowledged that only applications related to asylum currently use biometrics to validate identity. USCIS intends to work with DHS to establish a biometric and biographic data collection standard that will be common to USCIS, the Department of State, CBP, and ICE. Separately, USCIS is in the preliminary stages of plans to collect biometrics from customers when they first apply for a benefit and to use the biometrics to verify identity during subsequent processes. USCIS anticipates using this model for the Temporary Worker Program.

OIG Evaluation: We concur with USCIS' action and regard the recommendation as resolved and open. In its action plan, USCIS should explain which benefits will be included as biometric collection is expanded and note the results of its preliminary planning. Coordination with DHS to ensure the compatibility and interconnectivity of USCIS, CBP, ICE, and Department of State biometric identity systems is a critical part of managing the entry and exit of immigrants and non-immigrants to the United States.

Recommendation 2: Establish a comprehensive, risk-based plan for the selection and completion of security checks.

USCIS Response: FDNS will prepare a plan to outline how, when, and for what benefits expansion of biometric checks should occur. They will base this

analysis on risk assessments and assign responsibilities, timelines, and milestones for the implementation.

OIG Evaluation: We concur with USCIS' action and regard the recommendation as resolved and open. In its action plan, USCIS should include documentation of the plan's progress.

Recommendation 3: Set measurable objectives for the conduct and completion of all security checks and reorganize management controls to ensure objectives are met.

USCIS Response: FDNS, in coordination with the Production Management Division, will work to establish acceptable quality levels. These two offices will use information in the Background Check System to measure compliance with the quality levels. USCIS commented that management controls embedded in automated systems are the most effective for ensuring security check completion. Future USCIS systems will include these controls. In addition, FDNS will review and consolidate all USCIS guidance on security checks. USCIS will also explore ways to improve program management information by tracking adjudication decisions in relation to security check results.

OIG Evaluation: USCIS' proposed actions, including establishing acceptable quality levels for all forms and improving management controls such as policy documentation, are responsive to the recommendation. The recommendation is resolved and open.

Recommendation 4: Implement the Background Check Analysis Unit in the Office of Fraud Detection and National Security.

USCIS Response: USCIS noted that FDNS has resolved all national-security-related IBIS hits since March 2005. FDNS's Background Check Analysis Unit reviews, tracks, analyzes, and resolves all name-vetted hits related to rational security.

OIG Evaluation: This recommendation is resolved and open. In its action plan, USCIS should discuss the organizational and staffing changes made in FDNS to support the additional mission of analyzing and resolving national security hits.

Recommendation 5: Implement an automated system that stores applicants' biometric information and supports its use in security checks.

Recommendation 6: Implement an automated system that supports running, documenting, reviewing, and monitoring security checks.

USCIS Response: USCIS will deploy the Biometric Storage System in the fourth quarter of FY 2006 and the Background Check System in the third quarter of FY 2006.

OIG Evaluation: USCIS' proposed actions are responsive to the recommendations, which are resolved and open.

Recommendation 7: Define accountability and timelines for implementing changes to the security check process that include the development of the plan for completion of security checks, check completion objectives, and reorganized management controls.

USCIS Response: As of September 19, 2005, USCIS designated FDNS as the lead on all security check-related activities. As discussed in recommendations 2, FDNS will develop the plan for security check completion.

OIG Evaluation: This recommendation is resolved and open. In its action plan, USCIS should note the timeline for completion of changes to the security check process discussed in its response to this report.

Appendix A
Purpose, Scope and Methodology

We evaluated the adequacy and efficiency of the security checks that USCIS conducts to help identify unqualified alien beneficiaries, particularly terrorists and criminal aliens, and to deny their applications for immigration benefits. We examined the security check processes and procedures USCIS uses to detect fraud and identify mala fide applicants. We assessed the scope and depth of the security checks that USCIS performs to identify whether there are gaps in coverage and opportunities for increasing coverage. We reviewed USCIS' implementation of the security checks to learn whether checks are completed, properly conducted, and concluded with timely denials and law enforcement/fraud referrals when appropriate. Finally, we examined the efficiency of USCIS' implementation of the security checks, including frequency of duplicate checks and resources required for processing.

We analyzed laws and regulations related to immigration benefits and security checks; USCIS documentation, including guidance, directives, SOPs, manuals, policy memoranda, training materials, quality assurance reports, and Internet websites; various reports from the GAO and DOJ and DHS OIG on immigration benefits processing, fraud and security checks, and the management of immigration programs; and other related reports and articles.

During our review we conducted over 125 interviews and teleconferences. The majority of the interviews took place during our site visits to three USCIS service centers, four district offices, two asylum offices, two application support centers, and two file storage facilities. We spoke with senior officials at USCIS headquarters and at the Department of State, FBI, the Directorate of Border and Transportation Security, ICE, EOIR, and US-VISIT.

As part of our data analysis, we sampled over 600 immigration and asylum files for evidence of security check completion. Focusing on applications USCIS approved in FY 2004, we selected a random sample of eight different form types for which USCIS does not provide monthly, national quality assurance checks. These included two asylum-related forms that receive 100 percent supervisory review of security check completion. Based on inspector judgment, we sampled approximately 300 forms at each of two sites: the National Records Center (five form types) and the Harrisonburg storage facility (three form types).

Our fieldwork was conducted from October 2004 to March 2005. The review was conducted under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency.

Appendix B
Management Response to Draft Report

OCT-06-2005 10:45

INS / MGT RES STAFF

202 514 8667 P.02/07

U.S. Department of Homeland Security
20 Massachusetts Avenue, NW
Washington, D.C. 20529



**U.S. Citizenship
and Immigration
Services**

To: Robert L. Ashbaugh
Assistant Inspector General
Inspections and Special Reviews

From: Robert C. Divine *RCD*
Acting Deputy Director

Date: OCT 5 2005

Re: Comments on OIG Draft Report: A Review of U.S. Citizenship and Immigration Services' Alien Security Checks

We appreciate the opportunity to review and comment on the subject report. As the report noted, we have made many changes over the past few years to improve the adequacy of security checks, detect applicants who pose risks to national security and public safety and ensure that benefits are granted only to eligible applicants. Security checks support the Department of Homeland Security's goal of ensuring the security and integrity of the immigration system. However, as discussed throughout the report, we need to improve how we conduct this process, in order to increase efficiencies and effectiveness. Your report has highlighted a number of areas where we need to improve to include consolidating the management of this function into one office, ensuring that guidance to the field is clear, updated and available, and monitoring compliance with such guidance. Fundamental to changing the process is the need for better automated tools which are currently completing development and which should provide the staff with needed and timely information. USCIS plans to continue to pursue the issue of obtaining automatic updates from other agencies if there are changes in a person's criminal history and national security considerations. Only with this can the Department, Congress, and the public be assured that we have information available to fully address the Department's goals.

Recommendation 1. Expand the use of biometric identification in security checks, as consistent with risk assessment.

Agree. As stated in the report only applications related to asylum use biometrics to validate identity. However, our plans for transforming the way we do business will emphasize the requirement for early biometric collection from which to confirm identity. In doing this, we will work with the Department to establish a standard to collect core biometrics and biographic data on our customers at their first contacts with the Department of State, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, or us. Until this can be done, we will collect the information

Appendix B
Management Response to Draft Report

OCT-06-2005 10:45

INS / MGT RES STAFF

202 514 8667 P.03/07

Robert L. Ashbaugh

Comments on OIG Draft Report: A Review of U.S. Citizenship and Immigration Services' Alien Security Checks

Page 2

for our customers when they first apply for a benefit, connect the customer's biometric to a unique account number, and use the biometric to verify customer identity for subsequent steps and services. We are in the preliminary stages of planning, but anticipate this concept will be used as the business model for the Temporary Worker Program.

Recommendation 2. Establish a comprehensive, risk-based plan for the selection and completion of security checks.

Agree: We have begun expanding the use of biometrics for conducting security checks to other applications. In January 2005, we began requiring Temporary Protected Status applicants to undergo a new fingerprint check regardless of prior status and in May 2005, the same requirement was applied to applicants seeking a replacement Alien Registration Card. Effective September 19, 2005, the Office of Fraud Detection and National Security, has been designated the lead on all security check-related activities within USCIS. This office will prepare a comprehensive plan that will outline how, when, and for what benefits expansion of the use of biometric checks should occur based on risk assessments that are already underway. This plan will assign responsibilities, timelines and milestones for implementation.

Recommendation 3: Set measurable objectives for the conduct and completion of all security checks and reorganize management controls to ensure objectives are met.

Agree. As discussed in the report, the most effective controls for ensuring that security checks are accomplished are embedded into an automated system, as is done with CLAIMS 4 and RAPS. As we move forward with our information technology modernization initiatives, this function will be a requirement within the automated process. Until this is accomplished, the Background Check System should allow management to monitor the initiation and completion of security checks. The Office of Fraud Detection and National Security will work with the Production Management Division to establish acceptable quality levels for existing processes and to continually measure compliance against such levels using information from the Biometric Check System.

With respect to ensuring consistent guidance is available, as part of the plan discussed above, the Office of Fraud Detection and National Security will take the lead in reviewing and consolidating all guidance within USCIS that addresses security checks. Finally, the report identified weaknesses in the program management information, or lack thereof, over this process. We agree that we cannot effectively track adjudication decision that resulted from information derived through the security check process. We will start exploring ways to accomplish this function.

Recommendation 4: Implement the Background Check Analysis Unit in the Office of Fraud Detection and National Security.

Agree. Since March 2005, USCIS has required all IBIS hits related to National Security be reported to the Office of Fraud Detection and National Security for resolution and release for adjudicative action. The Background Check Analysis Unit was recently created to review, track, and analyze information submitted under a revised National Security Notification process. In this process, all name-vetted hits

Appendix B
Management Response to Draft Report

OCT-06-2005 10:46

INS / MGT RES STAFF

202 514 8667 P.04/07

Robert L. Ashbaugh

Comments on OIG Draft Report: A Review of U.S. Citizenship and Immigration Services' Alien Security Checks

Page 3

related to national security are forwarded to the Background Check Analysis Unit for review and resolution.

Recommendation 5: Implement an automated system that stores applicants' biometric information and supports its use in security checks.

Agree. As mentioned in the report, the Biometric Storage System will retain fingerprints, photographs and signatures for screening. This system will be deployed in the fourth quarter, FY 2006.

Recommendation 6: Implement an automated system that supports running, documenting, reviewing, and monitoring security checks.

Agree. The Background Check System will centralize records checks, reducing duplication of checks and supporting check reviews. The Background Check System will be deployed in the third quarter, FY 2006.

Recommendation 7: Define accountability and timeliness for implementing changes to the security check process that include the development of the plan for completion of security checks, check completion objectives, and reorganized management controls.

Agree. As discussed in the comments provided for recommendation 2, the Office of Fraud Detection and National Security will develop such a plan.

We want to express our appreciation to Wynne Krause and her team for the work they did in this highly critical and complex area. If you have any questions please contact Kathleen Stanley, USCIS Audit Liaison, at 202-272-1982.

Appendix C
Security Checks for USCIS Immigration Forms

Figure 4: Security Checks for USCIS Immigration Forms

FORM TITLE	FY 2004 Application Receipts ⁴¹	FY 2004 Application Completions ⁴²	IBIS Name Check	FBI Finger- print Check	FBI Name Check	IDENT Asylum
I-765 <i>Application for Employment Authorization</i>	1,555,176	1,919,980	yes			
I-90 <i>Application to Replace Permanent Resident Card</i>	624,583	1,111,469	yes	yes		
I-130 <i>Petition for Alien Relative</i>	712,320	831,042	yes			
I-485 <i>Application to Register Permanent Residence or to Adjust Status</i>	605,505	742,333	yes	yes	yes	
N-400 <i>Application for Naturalization</i>	662,788	639,377	yes	yes	yes	
I-131 <i>Application for Travel Document</i>	437,441	557,193	yes			
I-129 <i>Petition for a Nonimmigrant Worker</i>	418,125	433,744	yes ⁴³			
I-539 <i>Application to Extend/Change Nonimmigrant Status (Supp A also)</i>	251,735	280,687	yes			
I-751 <i>Petition to Remove the Conditions on Residence</i>	175,324	137,875	yes			
I-821 <i>Application for Temporary Protected Status</i>	13,826	126,493	yes	yes		
I-589 <i>Application for Asylum and Withholding of Removal</i>	32,859 ⁴⁴	110,646	yes	yes	yes	yes
I-140 <i>Immigrant Petition for Alien Worker</i>	80,348	85,844	yes			
N-600 <i>Application for Certification of Citizenship</i>	57,803	66,513	yes			
I-824 <i>Application for Action on an Approved Application or Petition</i>	29,140	37,253	yes			
I-881 <i>Application for Suspension of Deportation or Special Rule Cancellation of Removal (NACARA)</i>	12,368 ⁴⁵	35,441	yes	yes	yes	yes

⁴¹ USCIS Performance Analysis System data.

⁴² USCIS Performance Analysis System data.

⁴³ Unnamed applicants on blanket petitions do not receive IBIS checks.

⁴⁴ RAPS data.

⁴⁵ RAPS data.

Appendix C
Security Checks for USCIS Immigration Forms

FORM TITLE	FY 2004 Application Receipts ⁴¹	FY 2004 Application Completions ⁴²	IBIS Name Check	FBI Finger- print Check	FBI Name Check	IDENT Asylum
I-730 <i>Refugee/Asylee Relative Petition</i>	26,715	33,377	yes			
N-565 <i>Application for Replacement Naturalization/ Citizenship Document</i>	29,405	30,740	yes			
I-600 <i>Petition to Classify Orphan as an Immediate Relative</i>	28,066	29,913	yes	yes		
I-102 <i>Application for Replacement/ Initial Nonimmigrant Arrival/ Departure Document</i>	20,231	23,343	yes			
I-360 <i>Petition for Amerasian, Widow(er), or Special Immigrant</i>	12,600	11,403	yes			
N-336 <i>Request for Hearing on a Decision in Naturalization Proceedings under section 336 of the Act</i>	9,659	10,100	yes			
I-817 <i>Application for Family Unity Benefits</i>	6,697	9,584	yes	yes		
I-698 <i>Application to Adjust Status From Temporary to Permanent Resident (IRCA applicants)</i>	226	944	yes			
N-300 <i>Application to File Declaration of Intention</i>	205	753	yes			
N-470 <i>Application to Preserve Residence for Naturalization Purposes</i>	579	537	yes			
I-914 <i>Application for T Nonimmigrant Status (supporting form -B, family form -A)</i>	566	507	yes	yes		
I-690 <i>Application for Waiver of Grounds of Excludability under sections 245A or 210 of the Immigration and Nationality Act</i>	393	316	yes			
I-829 <i>Petition by Entrepreneur to Remove Conditions</i>	123	310	yes			
I-526 <i>Immigrant Petition By Alien Entrepreneur</i>	247	290	yes			
I-694 <i>Notice of Appeal of Decision</i>	155	248	yes			
I-914A <i>Application for T Nonimmigrant Status (family form -A)</i>	86	117	yes	yes		
N-644 <i>Application for Posthumous Citizenship</i>	9	3	yes			

Appendix C
Security Checks for USCIS Immigration Forms

FORM TITLE	FY 2004 Application Receipts ⁴¹	FY 2004 Application Completions ⁴²	IBIS Name Check	FBI Finger- print Check	FBI Name Check	IDENT Asylum
I-192 <i>Application for Advance Permission to Enter as Nonimmigrant</i>	data not available	data not available	yes	yes	yes	
I-212 <i>Application for Permission to Reapply for Admission into the U.S. After Deportation or Removal</i>	data not available	data not available	yes			
I-600A <i>Application for Advance Processing of Orphan Petition</i>	data not available	data not available	yes	yes		
I-601 <i>Application for Waiver of Grounds of Excludability</i>	data not available	data not available	yes	yes	yes	
I-602 <i>Application By Refugee For Waiver of Grounds of Excludability</i>	data not available	data not available	yes			
I-612 <i>Application for Waiver of the Foreign Residence Requirement</i>	data not available	data not available	yes			
I-94 <i>Arrival-Departure Record</i>	data not available	data not available	yes			

In addition to security checks performed on people, USCIS may conduct security checks on businesses (for example, those submitting an I-129, *Petition for Nonimmigrant Worker*) and schools (for example, those submitting an I-17, *School Approval*).

Appendix D
Major Contributors to Report

Office of Inspections

Douglas Ellice, Chief Inspector
Randall Bibby, Chief Inspector
David M. Hiles, Chief Inspector
Wynne Krause, Inspector
Kirsten Murray, Inspector
Melissa Keaster, Inspector

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretariat
Under Secretary, Border and Transportation Security
Director, Bureau of Citizenship and Immigration Services
Assistant Secretary, Public Affairs
Assistant Secretary, Legislative Affairs
Assistant Secretary of Policy
Deputy Chief Security Officer
OIG Audit Liaison
CIS Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Program Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; or write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.