U.S. Department of Justice
Office of the Inspector General
Evaluation and Inspections Division

Follow-up Review of the Status of IDENT/IAFIS Integration

Report Number I-2005-001

December 2004

EXECUTIVE SUMMARY

United States immigration authorities have long recognized the need for an automated fingerprint identification system to quickly determine the immigration and criminal histories of aliens they apprehend. However, the inability of immigration and law enforcement fingerprint identification systems to share information prevents law enforcement agencies from identifying criminals and wanted aliens in their custody, and has led to tragic results in some cases. In a report issued earlier this year, the Office of the Inspector General (OIG) described one such case, where border authorities twice released a man attempting to enter the country illegally. He subsequently returned to the United States illegally and traveled to Oregon where he raped two nuns, killing one. Because the federal government's immigration and law enforcement fingerprint databases were not linked, the immigration agents who stopped and released him at the border never learned of his extensive criminal record. See OIG report entitled "IDENT/IAFIS: The Batres Case and the Status of the Integration Project," March 2004 (Batres report).

Congress has expressed increasing concern that the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS) and the Department of Homeland Security's (DHS) Automated Biometric Identification System (IDENT) have not been integrated. After the terrorist attacks of September 11, 2001, Congress required that the fingerprint identification systems of law enforcement agencies be made interoperable so that criminals and known or suspected terrorists can be more readily identified.

In the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), which amended several key portions of the USA PATRIOT Act (Patriot Act), Congress required a "cross-agency, cross-platform electronic system that is a cost-effective, efficient, fully interoperable means to share law enforcement and intelligence information necessary to confirm the identity of…persons applying for a United States visa…."[1] The Patriot Act further required that this system be "readily and easily accessible" to all consular offices, federal inspection agents, and law enforcement and intelligence officers responsible for investigating aliens. The Border Security Act, in its description of an "interoperable data system," requires that immigration authorities have "current and immediate" access to information in federal law enforcement

[1] USA PATRIOT Act (P.L. 107-56), Section 403(c)(2).

agencies' databases in order to determine whether to allow aliens to enter the United States.[2]

During the past four years, the OIG has issued four reports that monitored the progress of efforts to integrate the automated biometric fingerprint systems of the DHS and the FBI.[3] In our most recent report, the March 2004 Batres report, we found that integration has been moving slowly and would take years to fully accomplish. Shortly after we issued the Batres report, however, the DHS committed to Congress that it would expedite deployment of the initial version of a workstation that integrates IDENT and IAFIS (Version 1.2 IDENT/IAFIS workstations). On September 21, 2004, the DHS reported that it had completed deployment of Version 1.2 to all 136 Border Patrol stations. In addition, DHS officials told us that the DHS is on schedule to complete deployment of Version 1.2 to 179 of the approximately 331 ports of entry by December 31, 2004.

The OIG initiated this review to determine if the Department of Justice (Department) and the FBI are prepared to support the increase in IAFIS queries expected to result from the DHS's expedited deployment of Version 1.2 workstations. However, because we discovered significant disagreements among the Departments of Justice, Homeland Security, and State regarding the definition and required elements of an interoperable biometric fingerprint system, we broadened our review to include an analysis of these issues. We also reviewed the status of the Department's efforts to develop and deploy the next planned version of IAFIS.

US-VISIT entry/exit system. In addition to effectively identifying criminals among apprehended illegal aliens, border authorities also intend to check visitors to the United States entering through ports of entry to ensure that they are not criminals or suspected terrorists. To accomplish this, the DHS is implementing a new entry/exit and border security system – the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) – at air, sea, and land ports of entry.

---

[2] Enhanced Border Security and Visa Reform Act of 2002 (P.L. 107-173), Section 202(a)(2).

[3] In March 2000, the OIG issued a report entitled "The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of its IDENT Automated Fingerprint Identification System"; a follow-up inspection report issued in December 2001 entitled "Status of IDENT/IAFIS Integration"; another follow-up inspection report issued in June 2003 entitled "Status of IDENT/IAFIS Integration"; and the March 2004 report entitled "IDENT/IAFIS: The Batres Case and the Status of the Integration Project." The INS was transferred to the Department of Homeland Security in March 2003.

To establish the entry/exit system quickly, the DHS designed US-VISIT to use IDENT and its biometric databases to collect two fingerprints and a digital photograph to provide the biometric identification for visitors. On July 18, 2003, the Homeland Security Council Deputies approved the use of a photograph and two fingerprints for initial US-VISIT deployment in sea and air ports of entry. At the same time, the Deputies directed the DHS and the DOS to work with the Homeland Security Council and the Office of Management and Budget in developing future plans to migrate to an eight fingerprint system. Consequent to the Deputies' decision, in September 2003, the DOS began to deploy small single finger scanners at its consulates and, in January 2004 the DHS launched US-VISIT. Both are based on the two-fingerprint system approved by the Deputies. The US-VISIT fingerprint checks against the IDENT database take approximately 15 to 20 seconds.

The DHS estimates that up to 43 million visitors a year – an average of about 118,000 per day – will be subject to the US-VISIT requirements.[4] This includes most visitors traveling to the United States on a visa and the nationals of the 27 countries participating in the Visa Waiver Program who do not require a visa if their stay for business or pleasure is less than 90 days.[5]

To ensure that US-VISIT is interoperable with IDENT/IAFIS, the Department of Justice, the DHS, and the Department of State (DOS) are working to establish the common elements of a comprehensive biometric fingerprint policy, as required by the Border Security Act. The Data Management Improvement Act of 2000 amended previous legislation requiring an entry/exit data system and required implementation deadlines for US-VISIT. The Border Security Act directed the Attorney General and Secretary of State to implement an entry/exit system that includes biometric identifiers which utilize a technology standard, and in recent legislation, Congress specifically directed that the biometric fingerprint systems operated by the Department

[4] The 118,000 projected daily visitors who submit two fingerprints and a photograph to US-VISIT do so at primary inspection, upon initial contact with immigration authorities. There are different procedures (described below) for those visitors referred to secondary inspection. Visitors are referred to secondary inspection if a search in any of the law enforcement/immigration databases queried at primary inspection results in a "hit" or if the person or their documents raise the suspicion of the primary immigration officer.

[5] Visitors not subject to US-VISIT requirements include those with certain designated visa classifications, children under the age of 14, persons over the age of 79, Mexican nationals to whom the Department of State has issued Border Crossing Cards for use along the southern border, and Canadians entering the United States across the northern border. Under the Visa Waiver Program, nationals of designated countries may enter and remain in the United States without obtaining a visa for up to 90 days.

and the DHS work together.[6] The DHS's appropriation bills for fiscal years (FY) 2004 and 2005 and the DOJ's FY 2005 appropriation bill specifically state that it is essential for US-VISIT to be interoperable with IAFIS (FY 2004), and for IDENT and IAFIS to ensure that both systems "can retrieve, in real time, biometric information contained in [IDENT and IAFIS] (FY 2005)."[7]

RESULTS IN BRIEF

This OIG review concluded that the FBI is prepared to handle the projected workload increase that will result from the DHS's expedited deployment of Version 1.2 IDENT/IAFIS workstations at Border Patrol stations and air, land, and sea ports of entry. We found that the DHS currently plans to use IAFIS to check the fingerprints of less than one percent of the visitors subject to US-VISIT at the ports of entry. However, if IAFIS will be required to search fingerprints of an expanded number of visitors, current and planned IAFIS capacity could be inadequate.

We also found that efforts to achieve the fully interoperable biometric fingerprint identification system directed by Congress have stalled. Despite months of effort, the DHS, the DOS, and the Department disagree on a uniform method for collecting fingerprint information or on the extent to which federal, state, and local law enforcement agencies will have direct access to biometric fingerprint records. The Department has warned that the federal government may face significant future costs to re-engineer the fingerprint identification systems if these issues are not resolved soon.

Meanwhile, the majority of visitors to the United States are still not checked directly against the FBI's IAFIS Criminal Master File, which is the most complete and current law enforcement database. Instead, the DHS continues to rely upon the interim measure of checking most visitors' fingerprints against the small portion of IAFIS data extracted into IDENT. As a result, criminal aliens – including many who committed violent crimes that threaten public safety – are not identified and prevented from entering the United States. In addition, the lack of immediate access to the FBI's full Criminal Master File creates a risk that a terrorist could enter the country undetected because the extract process results in a delay of up to one month

[6] After the DHS's creation in the Homeland Security Act of 2002, the responsibility for immigration-related issues (including US-VISIT) shifted from the Attorney General to the Secretary of the DHS.

[7] See DHS Appropriations Bills for FY 2004 (Conference Report 108-280) and FY 2005 (Conference Report 108-774), and DOJ Consolidated Appropriations Act, 2005 (Conference Report on H.R. 4818).

before new records of known or suspected terrorists' fingerprints are entered into the IDENT and US-VISIT databases.

For the Department of Justice to effectively proceed with its plans to make IAFIS interoperable with the biometric fingerprint systems of the DHS and the DOS, high-level policy decisions must be made regarding who should be subjected to fingerprint searches, the fingerprint collection standards to be used, the databases to be queried, who will have access to the information, how the information will be used, and who will maintain the databases.

Impact of projected DHS workload on IAFIS. The current and planned IAFIS capacity is sufficient to handle the projected workload that will result from the DHS's deployment of Version 1.2 of IDENT/IAFIS workstations. According to DHS projections, as of December 31, 2004, the DHS will conduct up to 6,400 full IAFIS checks (that do not rely on the IAFIS extracts) each day from ports of entry and Border Patrol stations nationwide. Our review indicates that current capacity of the FBI's IAFIS system will support up to 8,000 full IAFIS checks by the DHS each day. Planned IAFIS improvements through October 1, 2005, will increase IAFIS capacity to support 20,000 full IAFIS checks from the DHS each day.

Although the current and planned IAFIS capacity is sufficient to meet the DHS's requirements, the DHS workload projections assume that only a limited number of visitors will be subjected to electronic checks directly against the full IAFIS Criminal Master File. According to data provided by US-VISIT officials, between July 1, 2003, and June 30, 2004, an average of about 22,350 individuals were referred to secondary inspection each day, and 1,811 of these individuals were not admitted to the United States for law enforcement or administrative reasons. DHS inspection policy states that "all subjects who are suspected of being inadmissible to the United States shall be queried through IDENT/IAFIS." However, according to the DHS, by the end of FY 2005, it expects to directly check only about 800 individuals each day (0.7 percent of the 118,000 visitors subject to US-VISIT daily) against the full IAFIS Criminal Master File.

The vast majority of visitors (99.3 percent) will be checked only against the US-VISIT watch list.[8] These persons will not be checked directly against

[8] The US-VISIT watch list includes the IDENT lookout records, the IDENT apprehension records with alerts, "Wants and Warrants" data extracted from IAFIS daily, records of individuals from countries with special registration requirements, and individuals with unknown or foreign birthplaces or prior arrests on immigration charges. Wants and Warrants refer to the Wanted Persons file of the National Crime Information Center.

the full IAFIS Criminal Master File, which, as we explain below, could result in a failure to identify criminals or terrorists. However, a decision to check all of the 22,350 visitors referred to secondary inspection directly against IAFIS could exceed the current and planned IAFIS capacity of 20,000 daily searches.

IAFIS availability. Our review of system availability data from November 2003 through April 2004 found that IAFIS did not meet its requirement that the entire system be available 99 percent of the time. During that six-month period, the system was available 96.3 percent of the time. On 70 occasions, (including scheduled and unscheduled outages), downtime lasted 30 minutes or more and, in some cases, hours at a time. During these outages, FBI responses to DHS fingerprint search requests were not timely and resulted in aliens' fingerprints not being checked against IAFIS. Further, IAFIS users were not always notified of system outages. The excessive downtime occurred because there is no backup system that can continue to process transactions to completion when IAFIS or its components are taken out of service for scheduled or unscheduled maintenance. The FBI is currently working to improve IAFIS availability and provide more timely notification to customers when the system is unavailable.

Progress toward full interoperability. Although new interim measures to improve border security have been implemented since issuance of our Batres report, our current review found that the longer-term effort to implement a fully interoperable biometric fingerprint identification system has stalled. We identified two principal barriers to further progress. First, the DHS and the DOS have not agreed to implement the January 2003 Technology Standard, developed by the National Institute of Standards and Technology (NIST), jointly with the Attorney General and the Secretary of State, at the direction of Congress, as the uniform method for collecting fingerprint information and for searching against large databases. The NIST research showed that ten "flat" fingerprints can be taken almost as quickly as two flat fingerprints and that ten flat fingerprints offered search accuracy rates approaching the traditional law enforcement standard of ten "rolled" fingerprints.[9] The NIST showed that taking ten flat fingerprints offered a technologically and operationally acceptable approach for the Departments of Justice, Homeland Security, and State to screen incoming visitors. Accordingly, the NIST-recommended Technology Standard is for ten flat fingerprints to be taken to add or "enroll"

[9] The law enforcement standard is to take fingerprints from all ten fingers by rolling and pressing each finger on either a scanner or a standard fingerprint record form (ten rolled prints). Fingerprints also may be taken without rolling the fingers (flat fingerprints) and from fewer than ten fingers. Prints taken by simultaneously pressing all fingers straight down are referred to as "slap" fingerprints.

individuals in databases and to conduct searches of the databases. The NIST further recommended that two flat fingerprints and a digital picture be used to verify the identity of a person against an existing record, but not for enrollment. Thus, the current US-VISIT fingerprint collection standard (two flat fingerprints for enrollment and database searches) is not consistent with the NIST-recommended Technology Standard.

The second barrier to achieving interoperability is that the DHS and the Department disagree on a method of implementing a fully interoperable system that provides federal, state, and local law enforcement agencies with the "readily and easily accessible" access to the IDENT database specified in the Patriot Act and in subsequent congressional legislation. Similarly, the DHS does not believe that the FBI or other law enforcement agencies should have access to US-VISIT records. The DHS maintains this position for several reasons, including concerns that the information in IDENT is incomplete and could be misinterpreted, and to protect the privacy of visitors enrolled in US-VISIT. Without direct access to the DHS's IDENT database, it is more difficult for federal, state, and local law enforcement agencies to identify illegal aliens they encounter.

Because these issues have not been resolved, the DHS continues to rely on records extracted from IAFIS into IDENT for most fingerprint searches of visitors at ports of entry nationwide. The extracted data represents only a small portion of the more than 47 million records in the IAFIS Criminal Master File. A Department study of the extracted data has shown that the extracts are prone to have errors and omissions that result in missed criminals. Further, the fingerprint file of "Known or Suspected Terrorists" is only transmitted to the DHS once a month. Consequently, criminals or terrorists could be missed by checks against the extracted records.[10]

In an August 2004 preliminary draft Metrics Study report, the Department examined IDENT/IAFIS transactions that occurred at Border Patrol stations and at secondary inspection in ports of entry to determine if access to IAFIS would result in identifying more criminal aliens.[11] The Department reported that almost three quarters (73.1 percent) of the criminal aliens encountered at Border Patrol stations and ports of entry were identified only by checking IAFIS, and would not have been identified by checking IDENT

[10] The file contains approximately 15,000 fingerprints of known or suspected terrorists, including military detainees held oversees.

[11] The study did not include fingerprints of visitors submitted through US-VISIT at primary inspection.

alone.[12] The results clearly showed that not checking aliens against IAFIS increases the risk that the United States will unknowingly admit criminal aliens.

The Department has proposed conducting a similar study on visitors enrolled in US-VISIT, but, as of October 22, 2004, the DHS had not yet agreed to do so. Finally, the DHS's decision to continue using two flat fingerprints rather than ten flat fingerprints makes direct searches against IAFIS impractical because two-fingerprint searches would significantly reduce the accuracy of IAFIS by increasing the number of false positives.[13] In addition, the cost of searching IAFIS with two flat fingerprints is 25 times greater than ten fingerprints and requires significantly more computer processing resources. The Department has argued that the federal government may face significant costs to re-engineer its fingerprint identification systems in the future to implement a uniform fingerprint technology standard and make all the systems fully interoperable.

Actions taken in response to prior OIG recommendations. The Department and the FBI have taken steps that were responsive to all but one of the recommendations we made in our March 2004 Batres report. The Department was unable to implement our first recommendation, which was to develop a memorandum of understanding (MOU) with the DHS to guide the integration of IAFIS and IDENT. Although the agencies have continued to work together to solve operational and technical problems of mutual concern, the MOU has not been developed because of fundamental disagreements between the Department and the DHS over the attributes of an interoperable biometric fingerprint system and the degree to which the systems should be consolidated or made interoperable. For the other four recommendations:

- The Department assigned responsibility to a senior official. The Department assigned responsibility for coordinating the IDENT/IAFIS integration project to the Department Chief Information Officer (CIO). The CIO has been actively involved in efforts to develop a biometric fingerprint system that will most effectively meet the security and law

[12] This is the second of two congressionally directed "Cost and Operational Effectiveness Assessments." The first Metrics Study report was issued on July 18, 2003.

[13] The false positive rate, or false accept rate, is the probability that the system will incorrectly determine that a search fingerprint and a file fingerprint are matches. This would occur if a traveler is mistakenly matched as a criminal hit. The false negative rate, or false reject rate, is the probability that the system will not identify a search fingerprint match when the match is in the system. This would occur if a criminal with a record in IAFIS is not identified when his or her fingerprints are searched.

enforcement needs of all concerned parties. His office also developed two options for a long-term interoperable solution.

- The Department pursued development of Version 2 of IDENT/IAFIS. The Department's Justice Management Division has continued to plan for Version 2 of IDENT/IAFIS. Version 2 is intended to provide IDENT apprehension and criminal history information to other federal, state, and local law enforcement agencies.[14] The FBI's planned Next Generation IAFIS also includes elements that will support Version 2 of IDENT/IAFIS. Also, on September 4, 2004, the Department issued a solicitation for "fast capture" fingerprint/palm print technology that will quickly capture ten rolled-equivalent fingerprints or palm prints with better image quality than current technologies and that is affordable and deployable in the near future.

- The FBI started providing Wants and Warrants to the DHS on a daily basis. As of May 17, 2004, the FBI made the Wants and Warrants extracts from IAFIS available to the DHS on a daily basis. Previously, these extracts were provided once every two weeks. The Department considers extracts an interim measure only.

- The DHS established procedures to ensure that IAFIS data is available to the Border Patrol. As part of the its expedited deployment of Version 1.2 workstations, the DHS established and issued written procedures that outline appropriate steps to ensure that IAFIS criminal histories of all aliens who have criminal records are provided to and reviewed by the Border Patrol.

Conclusion. Notwithstanding the significant positive steps taken to expedite the deployment of the initial integrated version of IDENT/IAFIS, progress toward the longer term goal of making all biometric fingerprint systems fully interoperable has stalled. The Department, the DHS and the DOS have not agreed on a uniform fingerprint Technology Standard nor agreed how to develop a fully interoperable system that provides law enforcement agencies with "readily and easily accessible" access to IDENT and US-VISIT immigration records as directed by Congress in the Patriot Act and in subsequent congressional legislation.

Because these capabilities have not been developed, over 99 percent of the visitors seeking admission to the United States under the US-VISIT

[14] This was planned before US-VISIT and may no longer be applicable. Progress has stalled and JMD is not actively pursuing this approach as it awaits further decisions.

provisions will only be checked against the US-VISIT watch list. Because that watch list relies on a limited number of records extracted from the IAFIS Criminal Master File, the checks will not be as complete as those made directly against the full 47-million-record IAFIS Criminal Master File. As the Department's Metrics Study showed, when only extracts are checked many criminal aliens – including many who committed violent crimes that threaten public safety – are not identified and may be unknowingly admitted to the United States.

For the Department to effectively proceed with planning to make IAFIS interoperable with the biometric fingerprint systems of the DHS and the DOS, high-level policy decisions must be made regarding who should be subjected to fingerprint searches, the fingerprint collection standard to be used, the databases to be queried, who will have access to the information, how the information will be used, and who will maintain the databases. We recommend that the Department seek to have the federal government address those decisions in a timely way. Until those decisions are made, we recommend that the Department:

1. Within 90 days of the enactment of the Department's FY 2005 appropriations act, report to the Homeland Security Council and Congress that the Department, the DHS, and the DOS have reached an impasse and cannot complete the MOU directed by Congress. The report should formally request that the Homeland Security Council or Congress decide on the adoption of the NIST Technology Standard and define the capabilities to be provided in the interoperable system;

2. Increase the transmission of the fingerprints of Known or Suspected Terrorists from the FBI to the DHS from monthly to at least weekly;

3. Request access to a random sample of data from US-VISIT and other relevant immigration biometric databases used for enforcement or benefit purposes for comparison to IAFIS in order to determine the risk posed by not checking all visitors against IAFIS;

4. Coordinate with the DHS to identify the capacity needed to conduct IAFIS searches on all visitors referred to secondary inspection and inform the Department's CIO how the capacity of IAFIS (now planned to be 20,000 searches by October 1, 2005) could be increased to handle that level of activity;

5. Develop options for the eventual upgrade of IAFIS to enable the system to conduct ten flat fingerprint searches on all US-VISIT enrollees and TPRS submissions from the Border Patrol; [15] and

6. Take steps to ensure that IAFIS meets its availability requirement of 99 percent.

[15] Ten-Print Rap Sheet (TPRS) refers to the criminal history file associated with an alien's fingerprints. Border Patrol agents and inspectors at ports of entry receive a TPRS response from IAFIS if an alien's fingerprints return a potential match to fingerprints in the IAFIS database.

TABLE OF CONTENTS

INTRODUCTION

The Office of the Inspector General (OIG) conducted this review to examine the Department of Justice's (Department) and the Federal Bureau of Investigation's (FBI) preparations to support the expedited deployment of the initial integrated version of the Department of Homeland Security's (DHS) Automated Biometric Identification System (IDENT) and the FBI's Integrated Automated Fingerprint Identification System (IAFIS). However, because we discovered significant disagreements between the Departments of Justice, Homeland Security, and State regarding the definition and required elements of an interoperable biometric fingerprint system, we broadened our review scope to include an analysis of these issues. We also reviewed the Department's plans to develop and deploy the next version of IAFIS, which will be required to complete the integration project.

In four reviews since 2000, the OIG has reported on the efforts to integrate IDENT and IAFIS. In those reports, we found that integration was moving slowly and would take years to accomplish fully. These reports were:

- March 2000 - "The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of its IDENT Automated Fingerprint Identification System;"

- December 2001 - "Status of IDENT/IAFIS Integration" (follow-up report);

- June 2003 - "Status of IDENT/IAFIS Integration" (follow-up report); and

- March 2004 - "IDENT/IAFIS: The Batres Case and the Status of the Integration Project."

Since our March 2004 report, the use of IDENT/IAFIS at air, sea, and land ports of entry has been expanded to meet new DHS entry/exit and border security requirements implemented in the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) system. These requirements include an entry/exit tracking system to collect, maintain, and share information on foreign nationals, including biometric identifiers. Several of the principal federal agencies that manage and use biometric databases, including the Department, the DHS, and the Department of State (DOS), are in the process of establishing the common elements of a comprehensive biometric fingerprint policy and its attendant procedures to meet the new requirements of the Enhanced Border Security and Visa Reform Act of 2002 (Border Security Act).

The Background section of this report provides a brief description of the IAFIS, IDENT, and US-VISIT systems; the efforts to integrate the IDENT and IAFIS systems; congressional direction regarding the interoperability of these biometric fingerprint systems; and the DHS's efforts to expedite the deployment of Version 1.2 of IDENT/IAFIS. The Background section also identifies each of the federal agencies involved in the IDENT/IAFIS integration and the sharing of biometric fingerprint information among these agencies.

The Results of the Review section is organized into three parts. Part I describes the FBI's short-term preparations for the DHS's expedited deployment of Version 1.2 of IDENT/IAFIS. Part II describes the barriers to further integration of IDENT and IAFIS, including differing positions on interoperability and the minimum elements required for an interoperable biometric fingerprint system, as defined by the National Institute of Standards and Technology (NIST). Part III describes the Department's progress on the recommendations in our March 2004 report.

To supplement the descriptions provided in the Background section, Appendix I contains a complete history of the IDENT and IAFIS systems, including summaries of our four prior reports and the efforts made by the DHS and the FBI to integrate the systems. Appendix II contains a list of acronyms used in this report.

BACKGROUND

Fingerprint Biometric Identification Systems

The IAFIS, IDENT, and US-VISIT systems were designed by three different agencies to provide biometric identification support for three separate purposes. The uses and basic operation of each system are described below, along with a brief summary of the effort to integrate IDENT and IAFIS.

IAFIS. IAFIS is the FBI's automated fingerprint identification system and criminal history file, operated by the FBI's Criminal Justice Information Services (CJIS) Division in Clarksburg, West Virginia. IAFIS contains digitized records of latent fingerprints (e.g., fingerprints found at crime scenes) and a Criminal Master File of more than 47 million sets of ten rolled fingerprints.[16] IAFIS also includes a Civil Subject Index Master File, which contains fingerprints of non-criminals (e.g., military, government, or authorized non-government personnel). IAFIS includes three major components: the Automated Fingerprint Identification System (AFIS), the Identification Tasking and Networking (ITN), and the Interstate Identification Index (III). The AFIS is the search engine that matches fingerprint images, the ITN maintains the fingerprint image repository and manages workflow processes, and the III contains textual criminal history information on arrests and dispositions of criminal subjects.[17]

IAFIS provides fingerprint identification and criminal history services to the law enforcement community and others needing access to such data through a network of integrated systems. According to the IAFIS System Requirements Definition (SRD) document, the FBI provides "user identification services" to: "(1) authorized customers located at the over 62,000 law enforcement and criminal justice service agencies; (2) others who have an authorized justification (such as members of Congress or United States citizens

[16] The law enforcement standard is to take fingerprints from all ten fingers by rolling and pressing each finger on either a scanner or a standard fingerprint record form (ten rolled prints). Fingerprints also may be taken without rolling the fingers (flat fingerprints) and from fewer than ten fingers. Prints taken by simultaneously pressing all fingers straight down are referred to as "slap" fingerprints.

[17] Textual queries are also sent through IAFIS via the National Crime Information Center (NCIC), which operates a national database of computerized information on individuals with active wants and warrants, stolen articles, vehicles, guns, license plates, and other data. Over 80,000 participating federal, state, and local law enforcement agencies submit information for wanted and missing persons to the NCIC.

requesting their own FBI record); and (3) FBI staff members who are identified as service providers [e.g., fingerprint examiners]."[18] The five basic user identification services provided by IAFIS are:

- Ten-print services for criminal and civil fingerprints. Ten-print fingerprint records are checked against the criminal fingerprint database to identify subjects of criminal investigations or to do civil background checks and provide the requesting law enforcement agency with rap sheets of potential matches.[19] Civil fingerprint database checks are not routine.

- Image request services. Criminal database searches attempt to match subjects by name, FBI number, or other information to identify a fingerprint record.[20] For potential matches, the requestor receives the subject's fingerprint image and an indication of whether a criminal photo or palm print is available. These requests are known as "IRQs."

- Document submission services. These services include providing requesters with documents, expunging records from the database, consolidating multiple records, entering death notices, and responding to requests from United States citizens for their FBI records.

- Subject search and criminal history request services. Searches of the civil and criminal master files conducted using a subject's name and physical and/or biographic descriptors.

- Latent print services. The Forensic Analysis Division, within the FBI Laboratory located in Quantico, Virginia, attempts to match unidentified fingerprints (such as those from crime scenes) with fingerprints of known individuals.

[18] IAFIS Systems Requirement Definition, October 31, 2003, p. 7.

[19] Rap sheet refers to the Record of Arrests and Prosecutions.

[20] The FBI number is a unique identification number assigned to each individual who has a criminal history record in the NCIC. An associated fingerprint record for the individual will have the same FBI number.

TPRS and CAR transactions. In 2001, the CJIS Division developed the special Ten-Print Rap Sheet (TPRS) transaction for the DHS. The CJIS Division designed the TPRS, which refers to the criminal history file associated with an alien's fingerprints, to return a response within 10 minutes. When a Border Patrol agent or an officer in secondary inspection at a port of entry transmits an alien's fingerprints to IAFIS, the system searches its Criminal Master File for a potential "hit" or match. If the alien's fingerprints generate a match in IAFIS, and the fingerprint scores (based on the number of matching points between the fingerprints) of a candidate are above a predetermined threshold, IAFIS returns the criminal history file to the officer and the system automatically verifies the match. If the alien meets the DHS's booking criteria, the alien is booked at the station or the port of entry, and the officer transmits a Criminal Answer Required (CAR) rolled ten-print transaction back to IAFIS. This CAR fingerprint record is then accessible to other law enforcement agencies when they query IAFIS.

Efforts to Integrate IDENT and IAFIS

Since the early 1990s, the FBI and the INS have been discussing and working toward integrating their fingerprint identification systems. The integrated system, IDENT/IAFIS, has been developed and deployed in successive versions that implement increasing capabilities. Deployment of the current version of IDENT/IAFIS (Version 1.2) began in the fall of 2003. The purpose of the Version 1.2 integrated workstation was to provide information from IAFIS to immigration authorities.

Using Version 1.2 workstations, immigration officers take ten rolled fingerprints and a digital photograph. The IDENT/IAFIS workstation uses the ten-print record to query IAFIS and simultaneously uses the prints of the two index fingers to query and enroll the alien in IDENT. The results of the two queries are generally available to the officers in less than 10 minutes. The next planned version of the IDENT/IAFIS integrated system is Version 2. The goal of Version 2, which has not yet been developed, is to share immigration information with federal, state, and local law enforcement. For a complete history of the integration project, see Appendix I.

IDENT. IDENT was developed by the former Immigration and Naturalization Service (INS) to track individuals apprehended for illegal border crossing and to identify recidivists for possible criminal prosecution.[21] The system matches two flat fingerprints from the right and left index fingers of detained aliens against similar fingerprint records contained in the following IDENT databases:

- Lookout database. The lookout database contains fingerprints, photographs, and basic information on aliens who have been previously

[21] On March 1, 2003, the INS was transferred to the DHS and its operational responsibilities divided among three bureaus: the Bureau of Customs and Border Protection (CBP), the Bureau of Immigration and Customs Enforcement (ICE), and the Bureau of Citizenship and Immigration Services (CIS).

deported or who have criminal records. As of June 2004, there were approximately 1 million aliens in the lookout database.

- Apprehension database. The apprehension database contains fingerprints and photographs of aliens who have been previously apprehended. The apprehension database lists the time, date, and circumstances of each apprehension, as well as information on aliens who may require special attention, such as for a medical condition. As of June 2004, there were approximately 6 million aliens in the apprehension database. The apprehension database also includes alert records that may require special attention at a subsequent encounter, such as a medical alert, an officer safety alert, or an alert that the alien has a prior removal from the United States.[22]

US-VISIT. At the direction of Congress, the DHS developed the US-VISIT entry/exit tracking system to "collect, maintain, and share information on foreign nationals, including biometric identifiers, through a dynamic system that determines whether the individual should be prohibited from entering the U.S.; has overstayed or otherwise violated the terms of her/his admission; should be apprehended or detained for law enforcement action; [or] needs special protection/attention (e.g., refugees)."[23] The US-VISIT program is designed to provide "end-to-end management of data on foreign nationals covering their interactions with U.S. officials before they enter, when they enter, while they are in the U.S., and when they exit."[24] As of November 15, 2004, the US-VISIT database contained the records (two fingerprints and a photograph) of over 10 million enrolled legitimate travelers to the United States.

Approximately 260 million foreign visitors seek admission to the United States annually. In 2005, about 43 million of these visitors (about 118,000 per day) will be subject to enrollment into US-VISIT. The 43 million visitors subject to US-VISIT include most individuals traveling to the United States on a visa and the nationals of the 27 countries participating in the Visa Waiver Program

[22] IDENT also contains an Asylum database of fingerprint records searched and enrolled only by immigration officers that process asylum claims, and a Border Crossing Card database of fingerprints searched and enrolled by DOS officials that process Mexican Border Crossing Card applications and a database of the fingerprint records of nonimmigrant aliens arriving from certain countries identified as presenting an elevated security concern. Applicants seeking admission to the United States under US-VISIT are not searched against the apprehension, asylum, or border crossing card databases. Also, US-VISIT uses the lookout capability of IDENT to check the travelers' biometrics.

[23] US-VISIT Fiscal Year (FY) 2004 Expenditure Plan, January 2004, p.1.

[24] US-VISIT Fiscal Year (FY) 2004 Expenditure Plan, January 2004, p.1.

who do not require a visa if their stay for business or pleasure is less than 90 days. Visitors not subject to US-VISIT requirements include those with certain designated visa classifications, children under the age of 14, persons over the age of 79, Mexican nationals to whom the DOS has issued Border Crossing Cards for use along the southern border, and Canadians entering the United States across the northern border.

The DHS designed the US-VISIT system to collect two flat fingerprints and a digital photograph, and to query databases (such as the US-VISIT watch list and, for some visitors who will be refused admission, IAFIS) to ensure that the individual applying for a visa or seeking entry to the United States does not have any criminal or immigration violations before they are permitted to enter this country.[25] The fingerprints are taken either at visa-issuing consulates overseas or at the ports of entry when the visitors arrive. According to the DHS Expenditure Plan, this pre-entry processing will establish one "gold standard" identity for each foreign national and will be used in all of his or her future travel to and from the United States.

The first time a visitor's fingerprints are taken, they are checked against the US-VISIT watch list and the visitor is enrolled into the US-VISIT database.[26] When visitors subsequently enter or exit the United States, their fingerprints are only matched against their own enrolled fingerprints (a "one-to-one" verification match) to confirm the visitor's identity. In fiscal year (FY) 2003 and FY 2004, the DHS spent approximately $700 million on US-VISIT. The DHS anticipates spending up to $15 billion on the program in the next ten years.

Congress Directed That Biometric Identification Systems Be Interoperable

Beginning in 1999, Congress expressed its concern that the biometric identification systems of the FBI and the INS could not communicate, resulting in the INS encountering criminal aliens wanted by the FBI and releasing them without knowing that they were wanted. As documented in prior OIG reports on the Rafael Resendez-Ramirez and Victor Manual Batres cases, the failure to identify these criminals while they were in INS custody sometimes led to tragic results.

[25] The US-VISIT watch list includes the IDENT lookout records, the IDENT apprehension records with alerts, "Wants and Warrants" data extracted from IAFIS daily, records of individuals from countries with special registration requirements, and individuals with unknown or foreign birthplaces or prior arrests on immigration charges. Wants and Warrants refer to the Wanted Persons file of the National Crime Information Center.

[26] Because immigration inspectors at primary inspection generally have less than a minute to inspect arriving visitors, a rapid response time is essential. A check of the US-VISIT watch list takes approximately 15 to 20 seconds.

In the USA PATRIOT Act (Patriot Act) enacted on October 26, 2001, Congress directed the Attorney General and the Secretary of State, jointly with the NIST, to develop a technology standard for verifying the identity of visa applicants.[27] Congress called for a "cross-agency, cross-platform electronic system that is a cost-effective, efficient, fully integrated means to share law enforcement and intelligence information necessary to confirm the identity of…persons applying for a United States visa…."[28] The Department, the DOS, and the NIST were directed to "develop and certify a technology standard that can be used to verify the identify of persons applying for a United States visa or such persons seeking to enter the United States pursuant to a visa for the purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name or such person seeking to enter the United States…." The Patriot Act also specified that the electronic system should be readily and easily accessible to all consular offices, Federal inspection agents, and all law enforcement and intelligence officers responsible for investigating aliens.

The Border Security Act, enacted on January 23, 2002, amended several key portions of the Patriot Act, including the sections regarding the identification of aliens. Section 202(a)(2) of the Border Security Act required an "interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien."[29] The Border Security Act also amended the Patriot Act by accelerating the deadlines and expanding the technology standard to be developed by the Department (now the DHS), the DOS, and the NIST (described in the paragraph above) to include "appropriate biometric identifier standards."[30] The Border Security Act also required that the Department (now the DHS) and the DOS implement the technology standard at United States ports of entry and overseas consular posts, and to "issue to aliens only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers."

[27] After the DHS's creation in the Homeland Security Act of 2002, the responsibility for immigration-related issues shifted from the Attorney General to the Secretary of the DHS.

[28] USA PATRIOT Act (P.L. 107-56), Section 403(c)(2).

[29] In its directive regarding the sharing of biometric fingerprint information among systems, Congress describes the operations of the systems as being "fully-integrated" or "interoperable." For purposes of this report, we consider these terms to have the same meaning.

[30] Enhanced Border Security and Visa Reform Act of 2002 (P.L. 107-173), Section 202(a)(4)(B).

In more recent legislation, Congress has become increasingly specific in directing that the biometric fingerprint identification systems operated by various federal law enforcement agencies work together. On April 20, 2004, Senator Judd Gregg, Chairman of the Commerce, Justice, State and the Judiciary Appropriations Subcommittee, which initially approved funding for the FBI's IAFIS, spoke about fingerprint compatibility and the continuing need for the DHS to become fully integrated with the FBI. Regarding the deployment of DHS's IDENT/IAFIS Version 1.2 workstations, Senator Gregg stated:

> Workstations are only a one-way solution. Workstations give DHS access to IAFIS, but they do not give law enforcement access to immigration records. FBI and State and local law enforcement believe there are situations that require access to immigration records.
>
> Five years have passed and $41 million has been provided and the systems are still not integrated. Extracting a sampling of IAFIS information every two weeks is not enough…even daily extracts cannot substitute real-time information or full interoperability. The extracts do not include criminal histories. The need for criminal histories was made apparent in the 2002 case of Victor Manual Batres.

In reports accompanying the DHS's FY 2004 and FY 2005 appropriations bills, Congress gave specific directions regarding the interoperability of the IAFIS, IDENT, and US-VISIT systems.[31] The Congress also urged increased coordination between the Department and the DHS, as shown in the following excerpts:

> DHS Appropriations Bill, FY 2004 (Conference Report 108-280): The conferees believe that the success of US VISIT depends on the effective integration of biometrics into its systems and operations. The biometric infrastructure being built must be a viable long-term solution fully interoperable with the FBI [IAFIS] that meets biometric standards of [NIST].
>
> DOJ Appropriations Bill, FY 2005 (Conference Report on H.R. 4818, Consolidated Appropriations Act, 2005): The conferees are troubled by the security gap on the nation's borders caused by delays in linking [IDENT]….and [US-VISIT] with criminal history data contained in the [FBI's IAFIS]…With

[31] The Department is still operating under a continuing resolution, thus the FY 2005 Appropriation Bill is not yet available.

> implementation of a new visa tracking system and enrollment of millions of visitors into US-VISIT, it is essential that the Federal Bureau of Investigation collaborate with the Directorate of Border and Transportation Security to ensure that IDENT and US-VISIT can retrieve, in real time, biometric information contained in the IAFIS database, and that the IAFIS database can retrieve, in real time, biometric information contained in IDENT and US-VISIT.[32]

The DHS Deployed Version 1.2 of IDENT/IAFIS Workstations to All Border Patrol Stations, and Committed to Deploying the Integrated Workstations at 179 Ports of Entry by December 31, 2004.

The March 2004 Batres report generated significant attention on the status of the integration project. In March 2004, approximately two months after the launching of US-VISIT, DHS officials announced plans for an expedited deployment of Version 1.2 IDENT/IAFIS workstations. In congressional testimony, DHS officials announced that the DHS was planning to expedite the deployment of Version 1.2 IDENT/IAFIS workstations to all Border Patrol stations and the 50 highest volume ports of entry by December 31, 2004.

During a March 4, 2004, hearing of the Homeland Security Subcommittee of the House Appropriations Committee, DHS Secretary Tom Ridge responded to questions regarding findings contained in the OIG's Batres report. When the Committee Chairman asked Secretary Ridge why the Border Patrol did not yet have instant access to the FBI's fingerprint records, Secretary Ridge responded, "…I think we can make a significant number of connections between the points of entry in the Border Patrol and the database this year with the dollars available in the budget. I think that can get us up to 65 to 70 percent of those connections."

It was unclear from Secretary Ridge's congressional testimony whether the "65 to 70 percent" referred only to the Border Patrol stations (there are currently 136 nationwide), or also included the 331 United States ports of entry.[33] According to US-VISIT Program Managers we spoke with, they interpreted Secretary Ridge's reference to "65 to 70 percent" as applying only to

[32] This language is almost identical to the language in the DHS FY 2005 Appropriations Bill, Conference Report 108-774.

[33] This includes 317 sites in the United States and 14 "pre-clearance" sites in other countries.

Border Patrol stations. While the DHS's overall goal was to deploy IDENT/IAFIS workstations at 70 percent of the Border Patrol locations by the end of the 2004 calendar year, they were likely to exceed this goal and deploy the workstations to all Border Patrol stations by December 31, 2004. These same Program Managers indicated that in addition to deploying IDENT/IAFIS workstations to all Border Patrol stations, the DHS would also deploy the integrated workstations to 179 ports of entry by December 31, 2004. The 179 ports of entry will include all air and sea locations and the 50 largest land ports of entry. The DHS plans to complete deployment by December 31, 2005, when it installs workstations at its ICE investigative offices, detention locations, and the remaining ports of entry.

On September 21, 2004, the DHS issued a press release announcing the early completion of the deployment of the integrated workstations to all Border Patrol stations. Thus, the 1.1 million aliens apprehended by Border Patrol agents annually will now be processed with Version 1.2 of IDENT/IAFIS.[34] The following table (Table 1) provides a brief chronology of relevant deadlines and actions taken by the Department, the DHS, and other entities prior to, and immediately following, the issuance the OIG Batres report in March 2004.

[34] Exceptions to the requirement include aliens under 14 years of age, over 79 years of age, and when the workload at a Border Patrol station is too great, in which case Border Patrol agents are only required to enter/enroll apprehended aliens into IDENT.

Table 1 Timeline of IDENT/IAFIS/US-VISIT Actions and Deadlines in 2004	
DATE	**ACTION OR DEADLINE**
January 1/5/04	DHS launches Increment 1 of US-VISIT at 115 airports and 14 seaports.
February 2/1/04	FBI's CJIS Division continues implementing IAFIS upgrades began in September 2003.
March 3/2/04	OIG publishes report, "IDENT/IAFIS: The Batres Case and the Status of the Integration Project."
March 3/4/04	DHS Secretary announces expedited deployment of IDENT/IAFIS to 70% of Border Patrol stations by 12/31/04.
April 4/20/04	Senator Gregg stresses need for DHS/DOJ system interoperability, citing lack of interoperability between US-VISIT and IAFIS.
May 5/9/04	DHS begins expedited rollout of IDENT/IAFIS workstations at Border Patrol stations.
May 5/17/04	FBI's CJIS Division begins providing extracts of IAFIS data (Wants and Warrants) to DHS on a daily basis, instead of bi-weekly.
May 5/19/04	NIST issues report on one-to-one verification using fingerprint matching.
June 6/2/04	DHS selects Accenture as US-VISIT prime contractor.
	NIST issues report on US-VISIT's fingerprint identification performance.
June 6/4/04	NIST issues summary report of 2003 fingerprint vendor technology evaluation.
August 8/27/04	JMD releases preliminary draft of its second Metrics Study report.
September 9/4/04	The Department, through NIJ, solicits input for ten-print "fast capture" fingerprint/palm technology initiative.
September 9/13/04	NIST issues summary of past research, reiterating its January 2003 recommendations to Congress that ten flat fingerprints be the enrollment standard for large biometric databases, and two flat fingerprints and a photograph be the standard for identity verification.
September 9/21/04	DHS completes deployment of IDENT/IAFIS workstations at all Border Patrol stations ahead of schedule.
September 9/30/04	DHS expands US-VISIT procedures to include visitors traveling under the Visa Waiver Program arriving at air and sea ports of entry.
October 10/26/04	DOS deadline for all visa issuing consulates to electronically transmit two fingerprints to query the US-VISIT watch list, per the Border Security Act.
November 11/15/04	DHS goal for US-VISIT and IDENT/IAFIS installation at 50 busiest land ports of entry.
December 12/31/04	Data Management Improvement Act of 2000 deadline for US-VISIT installation at 50 busiest land ports of entry and DHS goal for IDENT/IAFIS installation at 180 ports of entry.

Key Agencies in the IDENT/IAFIS Integration

In response to the March 2004 OIG report on the Batres case and the status of the efforts to integrate IDENT and IAFIS, several other agencies, notably the DOS and the Department of Defense (DoD), have become more involved with the Department and the DHS as they decide how fingerprint biometrics should be collected and shared across the government. These agencies have also increased their coordination and communication with each other through participation in various interagency meetings. The following section describes each organization's role in the IDENT/IAFIS integration, and the interagency meetings held to support the project.

Department of Justice

Justice Management Division. The Justice Management Division (JMD) is the Department component with direct responsibility for the IDENT/IAFIS integration project. JMD has had oversight of the integration project since 1999, when the Attorney General assigned JMD to coordinate the development of a plan to integrate IDENT and IAFIS.[35] The Assistant Attorney General for Administration heads JMD, along with four Deputy Assistant Attorneys General (DAAG).

Management and Planning Staff. Within JMD, the Management and Planning Staff, under the DAAG for Policy, Management, and Planning, is responsible for the day-to-day coordination of the IDENT/IAFIS integration project. The Management and Planning Staff is responsible for compiling budget requests, creating project plans, conducting integration studies, publishing reports, attending regular interagency meetings, and working directly with Department and non-Department representatives on IDENT/IAFIS integration issues.

Office of the Chief Information Officer. The DAAG for Information Resources Management is the Department's Chief Information Officer (CIO), and is responsible for leading and implementing the efficient acquisition and management of information technology across the Department. The CIO is the highest ranking individual in the Department directly responsible for managing the IDENT/IAFIS integration project. The CIO represents the Department in meetings with the DHS and at high-level policy meetings with other non-Department entities, such as the Office of Management and Budget, the White House Homeland Security Council Deputies, and the CJIS Division.

[35] In July 1999, a House Report directed the INS to suspend further deployment of IDENT until the Department submitted a plan for integrating IDENT and IAFIS.

Joint Automated Booking System (JABS) Program Management Office. The purpose of the JABS is to enable federal law enforcement agencies nationwide to share information on offenders, including fingerprint data. The system receives booking information from law enforcement agencies, stores it, then queries IAFIS for matching fingerprint and biographical data. The JABS Program Management Office ensures that all Department law enforcement components, the DHS, and other federal agencies have access to JABS data, and also oversees the data sharing process.[36] The JABS Board of Directors is an oversight group for the JABS program that makes process and policy-related recommendations to the JABS Program Management Office.

FBI's Criminal Justice Information Services Division. The FBI's CJIS Division, located in Clarksburg, West Virginia, maintains and operates IAFIS. The CJIS Division has approximately 2,400 employees organized into the following three branches: Policy, Administrative and Liaison; Communications and Technology; and Operations. The Deputy Assistant Director (DAD) for the Operations Branch is responsible for identifying the funding needs of the various Operations Branch's priority projects and tasks. For the IDENT/IAFIS integration project, the Operations Branch DAD also serves as the FBI's liaison for policy issues with JMD, the DHS, and technical groups outside the FBI. Two of the Operations Branch's sections have direct responsibility for IAFIS -- the Information Technology Management Section (ITMS), and the Identification and Investigative Services Section (IISS).

Within the ITMS, the Requirements Management Unit (RMU) is responsible for identifying IAFIS user needs, developing system specifications, and conducting system testing. The RMU Chief works with other ITMS Unit Chiefs regarding IAFIS-related operations, systems, and technology support issues. The RMU Chief also serves as the technical liaison representing the CJIS Division at regular working group meetings with JMD and DHS staff. The IISS Chief attends meetings with JMD, the DHS, and other entities outside the FBI. The IISS houses the Division's approximately 250 fingerprint examiners who, when needed, verify fingerprint matches run through IAFIS. The fingerprint verification service is provided 24 hours a day, 7 days a week.

[36] All TPRS transactions pass through JABS. Therefore, JABS will also have to be prepared to support the increased workload from the DHS. The officials we spoke to stated that JABS was ready for the expedited deployment of Version 1.2.

Department of Homeland Security

On March 1, 2003, the DHS assumed responsibility for national border security and enforcement of immigration laws. The DHS has five major divisions or "directorates." The largest one, the Border and Transportation Security (BTS) Directorate, manages the IDENT and US-VISIT systems. The DHS's operational immigration responsibilities are divided among three bureaus: the Bureau of Customs and Border Protection (CBP), the Bureau of Immigration and Customs Enforcement (ICE) (both units of BTS), and the Bureau of Citizenship and Immigration Services (CIS).

Bureau of Customs and Border Protection. The Border Patrol falls under the DHS's CBP, along with employees from the former U.S. Customs Service, the INS, and the Department of Agriculture. The CBP's mission includes preventing terrorists and criminal aliens from entering the United States and apprehending individuals attempting to enter the United States illegally. Over 40,000 employees, including Border Patrol agents and inspectors stationed at ports of entry, work for the CBP.

US-VISIT Program Management Office. The DHS manages US-VISIT through its US-VISIT Program Management Office. The Office includes the ENFORCE/IDENT Program Management Office, which in turn manages IDENT/IAFIS integration and deployment of integrated workstations.[37] The Program Management Office staff's responsibilities include communicating with CJIS Division and JMD representatives and participating in meetings with non-Department entities.

Biometrics Support Center. The Biometrics Support Center is a DHS contractor facility that updates and maintains the IDENT lookout and apprehensions with alert database enrollments. It also provides DHS agents with an immediate response to (non-electronic) queries of subjects' fingerprints. The Biometrics Support Center is staffed with fingerprint examiners, many of whom are former FBI personnel. The Biometrics Support Center also accepts search requests from local law enforcement personnel through a local immigration officer.

[37] ENFORCE is the DHS's case management system that documents and tracks the investigation, identification, apprehension, detention, and removal of immigration law violators.

National Institute of Standards and Technology

The Commerce Department's NIST has statutory authority, along with the Secretaries of State and Homeland Security, to develop and certify a Technology Standard that includes biometrics, in order to verify the identity of individuals applying for a visa or using a visa to enter the United States. In developing this Technology Standard, the NIST evaluated government and commercial biometric systems, and published the results of its research, including recommendations, in several reports since 2002. Scientists at the NIST have been working with the FBI for over 30 years to research, develop, and improve fingerprint-matching procedures, and have created several fingerprint databases used to test new fingerprint identification algorithms and "live" fingerprint scanners, such as the types used by US-VISIT and IDENT/IAFIS. The NIST works with representatives from the CJIS Division, JMD, the DOS, and the DHS, and participates in regular interagency meetings with them and relevant contractors.

Department of State

To comply with the US-VISIT biometric identifier requirement, the DOS is currently deploying small single-finger electronic fingerprint scanners and digital cameras at all United States visa processing embassies and overseas consulates. The DOS US-VISIT deployment schedule indicates that, as of October 26, 2004, all of the approximately 214 visa-issuing consulates are required to transmit two flat fingerprints to query the IDENT/US-VISIT biometric watch list.[38]

Bureau of Consular Affairs. The DOS's Bureau of Consular Affairs is responsible for implementing policies relating to the broad range of overseas consular services and immigration, including the management of individuals applying for a United States visa. Representatives from the Bureau of Consular Affairs work with the DHS and the Department regarding biometrics issues, and participate in the interagency meetings regarding fingerprint issues. The Bureau of Consular Affairs is also overseeing several pilot projects with the FBI, in which United States consulates in Mexico (including Guadalajara and Monterrey) are taking ten flat fingerprints from visa applicants.

[38] This deadline, postponed from October 1, 2003, refers to the date by which certain passports used for travel to the United States must be machine-readable (Border Security Act, Section 303).

Department of Defense

The Secretary of the Army is responsible for biometrics within the DoD. The Army's Biometric Management Office and Biometrics Fusion Center report directly to the Army CIO.

Biometric Management Office. Representatives from the DoD's Biometric Management Office have been working with FBI's CJIS Division since November 2003 to develop standardized policies for collecting, searching and sharing fingerprints collected overseas from military detainees and latent fingerprints gathered from investigation sites. As a result of this collaboration, the DoD is currently upgrading its technology to conform to the electronic fingerprint standards that IAFIS utilizes. The DoD is in the process of configuring its own automated fingerprint identification system and is coordinating with the CJIS Division. The Biometric Management Office representatives also participate in various inter-agency meetings.

Key Working Groups

The above groups have created several interagency committees and working groups to coordinate the sharing of biometric fingerprint information. They address topics ranging from policy and long-term issues, to meetings with working-level participants to discuss technical and operational issues. The committees and working groups include:

- **Executive Office of the President, Homeland Security Council, Deputies Committee.** Officials at the Deputy level (or their designees) from the Department, the DHS, the DOS, and other agencies have met regularly since January 2004 to discuss security issues, including IDENT/IAFIS and US-VISIT fingerprint biometric interoperability issues and long-term goals.

- **Policy Coordination Committee.** Also formed in January 2004, the Policy Coordination Committee reports to the Homeland Security Council Deputies on issues such as current and future use of the fingerprint data contained in IAFIS, IDENT, and US-VISIT. Managed by the Office of Management and Budget, Policy Coordination Committee participants include representatives from the Department (e.g., the CIO, the FBI CJIS Division, and JMD), the DHS, the DOS, and the DoD.

- **US-VISIT Federal Stakeholders Advisory Board (US-VISIT Board).** The US-VISIT Board, chaired by the DHS's Under Secretary for BTS, provides advice and recommendations for the management of the US-VISIT system. Non-DHS members include the Department CIO, Assistant

Director in Charge of the CJIS Division, and the Deputy Assistant Secretary of State for Consular Affairs.

- **Interagency Task Force**. The Task Force, chaired by the Director of US-VISIT, meets weekly to discuss operational issues but has no policy role. The group includes Accenture (US-VISIT prime contractor) and representatives from across the DHS and other agencies. The Department's Office of the CIO is also represented.

- **US-VISIT Strategic Plan Team**. The Team outlines business requirements needed for immigration and border management and the technology, data, and facilities needed to support the requirements. The FBI CJIS Division and the Department are represented.

- **NIST Biometric Working Group.** Representatives from JMD, CJIS Division, the DOS, the DHS, as well as relevant contractors, attend regular meetings at the NIST to discuss issues surrounding Patriot Act biometrics. Scientists at the NIST attend these meetings and explain to participants the findings of their biometrics research studies.

- **JABS Board of Directors.** The JABS Board of Directors is an oversight group that makes process and policy-related recommendations to the JABS Policy Management Office. It is comprised of the Department's CIO, a Section Chief from the CJIS Division, and other representatives from the organizations that utilize JABS.

- **Source Selection Advisory Committee.** The DHS formed the Source Selection Advisory Committee, which was comprised of managers from the DHS's US-VISIT Policy Management Office and included the CJIS Division's Operations Branch DAD, to select the prime contractor for US-VISIT. The contract was awarded to Accenture on June 2, 2004.

SCOPE AND METHODOLOGY

Because the scope of this review involves issues beyond the Department, including issues within the DHS, we coordinated this review with the DHS's Office of Inspector General. Our fieldwork consisted of interviews, site visits, and extensive documentation review.

Interviews. We interviewed individuals from the Department, the DHS, the NIST, the DOS, and the DoD. We also spoke to contractors working for the companies responsible for supporting the integration project.

Interviews with Department personnel. From the Department, we interviewed the CIO, his Special Assistant, and a Senior Program Analyst in the CIO's office. From JMD, we interviewed the IDENT/IAFIS and JABS Program Managers, and members of their staff. From the FBI, we interviewed the Assistant Director in Charge of the CJIS Division and members of his staff, including two Deputy Assistant Directors, two Section Chiefs, a Senior Information Technology Specialist, a fingerprint examiner, and several other senior personnel at the CJIS Division.

Interviews with DHS personnel. From the DHS's US-VISIT Program Management Office, we interviewed the Deputy Director of US-VISIT, and several IDENT/IAFIS Program Managers. From the Bureau of Customs and Border Protection, we interviewed the senior Border Patrol Officer responsible for IDENT/IAFIS, an inspector at the Dulles International Airport, and a Program Officer from the executive office of US-VISIT.

Interviews with the NIST, the DOS, and the DoD. From the NIST, we interviewed the chief scientist with principle responsibility for biometrics research. From the State Department, we interviewed the Deputy Assistant Secretary of State for Consular Affairs, and two members of her staff involved in biometrics. From the Defense Department, we interviewed the Director of the DoD Biometrics Management Office, a representative of the DoD's Office of the Assistant Secretary of Defense, and several contractors.

Site visits. We visited the FBI's CJIS Division in Clarksburg, West Virginia in order to interview FBI personnel and observe IAFIS system capabilities. We also visited the DHS's port of entry at Dulles International Airport to observe IDENT/IAFIS operations and US-VISIT entry/exit procedures, and to interview DHS staff. In addition, we attended the Department's Fingerprint Vendor Technology Evaluation meeting, and a presentation given by JMD and relevant contractors regarding their assessment of IDENT/IAFIS search accuracy.

Documentation review. We reviewed numerous documents, including the Department's and the DHS's updated deployment and budget plans; the most recent JMD Metrics Study; fingerprint biometrics studies conducted by the NIST and the FBI; IDENT/IAFIS integration status reports; recent congressional testimony and reports; FBI and US-VISIT system descriptions and performance data; interagency meeting minutes; and correspondence between representatives from the Departments of Justice, Homeland Security, and State.

Existing FBI IAFIS capacity is sufficient to handle the projected workload increase that will result from the DHS's expedited deployment of Version 1.2 of IDENT/IAFIS workstations. However, that conclusion is based on current DHS workload projections which assume that less than one percent of visitors will be subjected to direct IAFIS fingerprint searches at the ports of entry. Current and planned IAFIS capacity through October 1, 2005, is not adequate to support a significant expansion of the number of visitors searched. In addition to having adequate current capacity, the FBI requires that the IAFIS system be available to users at least 99 percent of the time. Between November 2003 and April 2004, IAFIS failed to meet system availability requirements. Because there is no backup system, during scheduled or unscheduled maintenance IAFIS must be taken out of service and cannot complete fingerprint searches. As a result, responses to DHS's fingerprint search requests were delayed, resulting in aliens' fingerprints not being checked against IAFIS at all. The FBI is working to improve system availability and provide more timely notification to customers when the system is unavailable.

Existing FBI IAFIS Capacity is Sufficient to Handle the Projected Workload Increase That Will Result From the DHS's Expedited Deployment of Version 1.2 of IDENT/IAFIS Workstations

On March 4, 2004, DHS Secretary Ridge testified before Congress that the DHS would expedite the deployment of Version 1.2 IDENT/IAFIS workstations. The DHS committed to completing deployment of the new workstations to all its Border Patrol stations and to the 179 ports of entry included in the first two phases of US-VISIT (the 115 air ports of entry, 14 sea ports of entry, and the 50 busiest land ports of entry) by December 31, 2004. As of September 21, 2004, the DHS completed deployment of Version 1.2 workstations to all 136 of its Border Patrol stations. DHS officials told us that they are on track to deploy Version 1.2 workstations to the 179 ports of entry by the end of 2004.

The deployment of Version 1.2 integrated workstations will increase the number of IAFIS queries submitted by the DHS. The DHS conducted an analysis to estimate the potential increase in TPRS queries that would be sent to IAFIS from all Border Patrol stations and all US-VISIT air, land, and sea ports of entry through December 31, 2005 (when the DHS is scheduled to complete deployment of the Version 1.2 workstations). As part of the analysis, the DHS included information on low and peak times of day and year. For January through April 2004, the DHS-projected number of daily transactions for the Border Patrol ranged from a low of 2,553 to a high of 5,230. For the ports of entry, the DHS-projected number of daily TPRS transactions ranged from a low of 629 to a high of 829.[39] Based on the DHS data, we estimated that the daily range of TPRS IAFIS queries after December 31, 2005, could be between 3,182 and 6,059 queries per day.

For other data on IAFIS workload and preparations to meet DHS requirements, we contacted CJIS Division officials. They told us that, as of May 25, 2004, the DHS was submitting approximately 2,200 to 3,000 TPRS search requests each day; 1,300 CAR bookings; and 3,000 fingerprint image requests to IAFIS (Table 2). At that time, IAFIS was capable of processing 8,000 TPRS requests per day.

Table 2 – IAFIS Daily Capacity and Usage

Query Types	CURRENT Capacity	CURRENT Queries (All sources)	CURRENT Queries (DHS Only)	Planned Version 1.2 Capacity (10/1/2005)	Projected Queries (All sources) (10/1/2005)	Projected Queries (DHS Only) (10/1/2005)
TPRS queries (DHS only)	8,000		2,200-3,000	20,000		3,182 – 6,059[a]
CAR bookings	30,000	20,500	1,300	60,000	35,000	up to 3,900[b]
IRQ	7,000	6,000	3,000[c]	7,000	6,000	3,000
Latents	635[d]	350	25	635	450	up to 158[e]
Name checks/III/ Criminal histories	850,000	425,000	187,000	850,000	470,000	Unknown

(a) Provided by the DHS. The DHS projection is based on workload data for January through April 2004.
(b) The FBI plans to support up to 1 million additional annual CAR bookings from the DHS after October 1, 2005.
(c) The CJIS Division limits the DHS to 3,000 IRQs per day to ensure that other entities have access to fingerprint image retrievals.
(d) All federal agencies except the FBI have been allocated 25 percent of IAFIS's latent fingerprint search capacity.
(e) The DHS allocation is 158; in the past the DHS has not submitted latent requests up to its allocation.

Source: CJIS Division, except where noted as from the DHS.

[39] The DHS projection assumed there would be 71 TPRS transactions for every 100 IDENT search and enroll transactions.

According to the CJIS Division's FY 2005 Budget Enhancement Request, as of May 2004 the CJIS Division had implemented $2.7 million worth of IAFIS improvements, including upgrades of the IAFIS server platform and network, expanded storage capacity, and increased bandwidth. After October 1, 2005, the CJIS Division expects to implement enhancements that will increase IAFIS capacity from the current 8,000 daily TPRS search requests to 20,000 daily TPRS search requests.[40] The CJIS also plans to increase its capacity to process CAR bookings from the current 30,000 to 60,000 per day. The increased CAR capacity will accommodate up to 1 million additional CAR submissions per year from the DHS. The capacity for fingerprint image requests and name checks will remain the same for FY 2005. The CJIS Division plans to hire additional fingerprint examiners (above the 12 requested in the FY 2005 budget request) to supplement the approximately 250 examiners already on board and support anticipated retirements.

In addition, the Budget Enhancement Request indicated that the CJIS Division is implementing several IAFIS upgrades in FY 2004 and FY 2005 to enable the FBI to better support the DHS. For example, the CJIS Division was planning to:

- Reduce the guaranteed IAFIS processing time for TPRS responses from 10 minutes to 2 to 3 minutes by prioritizing TPRS transactions; and

- Provide additional software and hardware upgrades to support these enhancements, including requesting an additional $12.4 million in IAFIS system enhancements for FY 2005 (that would represent the bulk of the FBI's FY 2005 IDENT/IAFIS budget of $16 million).

Based on the existing IAFIS capacity of 8,000 TPRS transactions per day, the FBI appears to be capable of handling the increased volume of TPRS searches projected to occur as a result of the DHS's expedited deployment of Version 1.2 of IDENT/IAFIS workstations through December 2004. The current capacity also appears capable of supporting a decision by the DHS to conduct a TPRS check on all of the aliens not admitted to the United States each day at the ports of entry. The planned IAFIS upgrades will increase the TPRS transaction capacity to 20,000 searches per day by October 1, 2005, and will give the system a surplus capacity of at least 13,000 TPRS transactions over the 6,059 maximum expected daily workload from the DHS.

[40] CJIS Division representatives met with the IAFIS contractor, Lockheed Martin, to ensure that they would be able to support 20,000 TPRS transactions per day. Operations and maintenance functions are managed by FBI staff and executed by FBI and Lockheed Martin staff.

DHS Workload Projections Assume That Less Than One Percent of Visitors Will Be Subjected to Direct IAFIS Fingerprint Searches at the Ports of Entry

Although we concluded that the FBI is prepared to meet the expected increase in IAFIS workload through October 1, 2005, we noted that DHS workload projections assume that the number of visitors who receive IAFIS fingerprint searches will be sharply limited. The DHS is not planning to use IAFIS TPRS searches to screen all, or even many, visitors at ports of entry, but plans to limit TPRS queries to a small percentage of those who are referred to secondary inspection and not admitted to the United States.[41] According to the DHS, in 2005 approximately 43 million visitors to the United States (an average of 118,000 each day) will be subject to US-VISIT requirements at ports of entry nationwide. The DHS estimates that, once full deployment of all IDENT/IAFIS workstations is complete, it will request direct TPRS IAFIS queries on about 800 aliens each day (0.7 percent of the visitors subject to US-VISIT). Although the 800 a day projection is significantly lower than the average of 1,800 individuals a day who were determined inadmissible between July 1, 2003 and June 30, 2004, present IAFIS capacity could handle an additional 1,000 queries a day.[42] The other 99.3 percent of aliens requesting entry into the United States will be checked against US-VISIT, but will not be checked against the IAFIS Criminal Master File.

If the number of visitors who are subjected to IAFIS fingerprint searches is expanded, the current and planned IAFIS capacity through October 1, 2005, may be exceeded. Although we concluded that current and planned IAFIS capacity is sufficient to meet the DHS's projected requirements, the DHS workload projections assume that only about 800 visitors will be subjected to IAFIS fingerprint searches at the ports of entry each day. That represents only 0.7 percent of the 118,000 total projected daily visitors in 2005 that are denied admittance each day. According to data provided by US-VISIT officials, between July 1, 2003, and June 30, 2004, an average of about 22,350 individuals referred to secondary inspection each day, and 1,811 of the individuals were not admitted to the United States for law enforcement or

[41] Visitors are referred to secondary inspection if a search in any of the law enforcement/immigration databases queried at primary inspection results in a hit or if they raise the suspicion of the primary immigration officer. DHS data for the period from July 1, 2003, to June 30, 2004, shows that 8,156,638 of the 260,863,839 visitors to the United States (8.9 percent) were referred by immigration agents for secondary inspection. Of these, 661,072 (0.3 percent of all visitors), or about 1,811 per day, were subsequently not admitted to the United States due to administrative, immigration, or criminal issues.

[42] DHS inspection policy states that "all subjects who are suspected of being inadmissible to the United States shall be queried through IDENT/IAFIS."

administrative reasons.[43] The vast majority of visitors subject to the provisions of US-VISIT (99.3 percent) will be checked against the US-VISIT watch list, which contains a limited number of records extracted from the IAFIS database such as the Wants and Warrants file, but the visitors will not be checked directly against the full IAFIS Criminal Master File.

Although by October 1, 2005 IAFIS will have surplus capacity of between 13,000 and 16,000 TPRS transactions over current projected requirements, the number of visitors checked directly against IAFIS could increase significantly if the population of visitors subjected to the IAFIS TPRS searches is expanded. For example, a decision to check all visitors referred for secondary inspection – which averaged 22,350 each day between July 1, 2003, and June 30, 2004 – could exceed the current and planned IAFIS capacity of 20,000 TPRS searches per day through October 1, 2005. Although such an expansion is not currently planned, this could change based on the results of a proposed study discussed later in this report that would determine how many criminal visitors missed by US-VISIT could have been detected by checking IAFIS.

Between November 2003 and April 2004, IAFIS Failed to Meet System Availability Requirements.

In addition to having the capacity to process its expected workload, the IAFIS system must be continually operational in order to respond to fingerprint search requests 24 hours a day, 7 days a week. However, the IAFIS system consists of several components that do not have redundant backup systems, so when any of the components is out of service for software or hardware upgrades (scheduled downtime), or due to unforeseen system problems (unscheduled downtime), the FBI cannot continue to fully process fingerprint search requests.[44] Availability requirements call for the entire IAFIS system to be available to users 99 percent of the time and for each IAFIS component to be available 99.5 percent of the time.

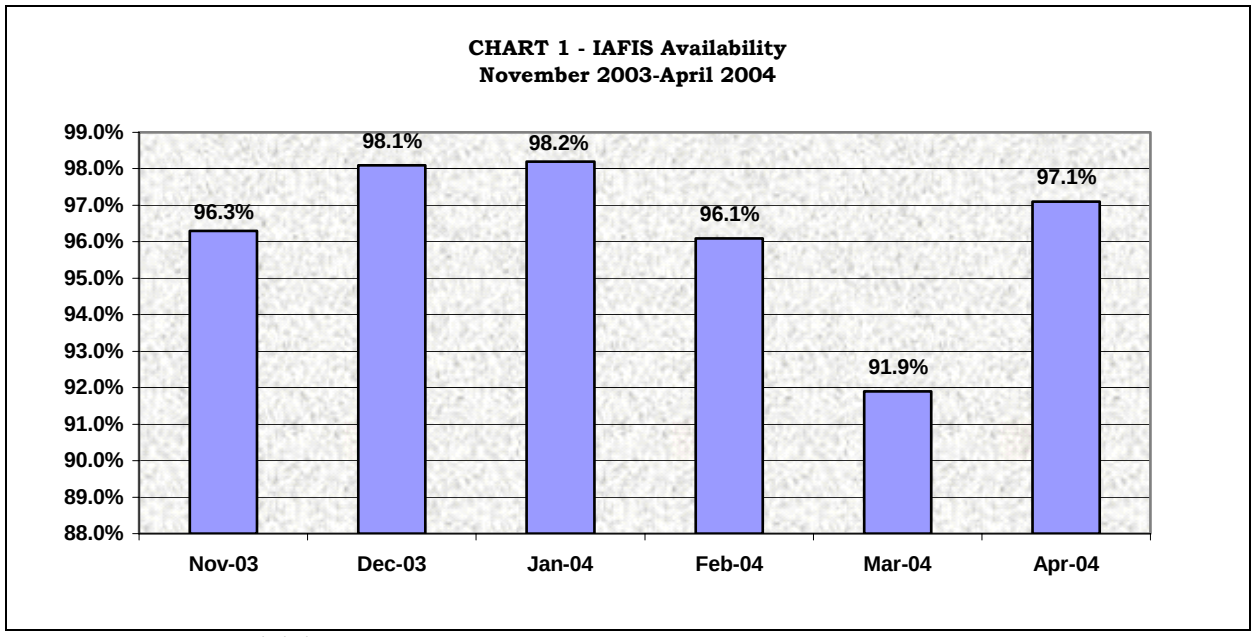
According to CJIS Division data, IAFIS has not been meeting these system availability requirements. We found that during the six months from November 2003 through April 2004, IAFIS was down a total of 161 hours, resulting in an average monthly availability of approximately 96 percent

[43] Visitors are referred to secondary inspection if a search in any of the law enforcement/immigration databases queried at primary inspection results in a hit or if they raise the suspicion of the primary immigration officer.

[44] Depending on the specific component that is out of service, queries can sometimes be partially processed by the available IAFIS components and queued until the remaining components are available.

(Chart 1). Of the 161 hours of downtime, about 60 percent was scheduled and 40 percent was unscheduled (Table 3, next page). During this six-month period, IAFIS had 24 scheduled outages and 46 unscheduled outages of 30 minutes or more.

Excessive downtime makes it possible for aliens with a criminal record in IAFIS but with no criminal record in IDENT to be released. The impact is most acutely felt at Border Patrol stations that are processing large numbers of apprehended aliens. If Border Patrol agents do not receive a response from IAFIS within 10 minutes or shortly thereafter, decisions on whether to detain or release the alien will be made based only on the results of an IDENT query. Visitors at ports of entry already will have been checked against the US-VISIT watch list, and, if they are referred to secondary inspection, officers can query the IAFIS criminal history database by the visitors' name and make a decision based on checks of other immigration databases. However, there is still the risk of not having the right name and missing information that would be available through a fingerprint match.



Source: FBI CJIS Division

TABLE 3 FBI IAFIS Availability for Six-Month Period November 2003 - April 2004								
Date	**Hours in Month**	**Downtime**		**IAFIS Availability**	**Unscheduled Downtime**		**Scheduled Downtime**	
		(Hours)	**(Percent)**	**(Percent)**	**(Hours)**	**(Percent)**	**(Hours)**	**(Percent)**
November-03	720	26:26	3.8%	96.2%	10:40	40.4%	15:46	59.6%
December-03	744	13:50	1.9%	98.1%	2:50	20.5%	11:00	79.5%
January-04	744	13:27	1.8%	98.2%	8:47	65.3%	4:40	34.7%
February-04	696	27:10	3.9%	96.1%	8:36	31.7%	18:34	68.3%
March-04	744	59:59	8.1%	91.9%	36:22	60.6%	23:37	39.4%
April-04	720	20:58	2.9%	97.1%	4:50	23.1%	16:08	76.9%
TOTAL	**4,368**	**161:50**	**3.7%**	**96.3%**	**72:05**	**40.4%**	**89:45**	**59.6%**

Source: FBI CJIS Division

CJIS Division officials told us that they schedule downtime periods of about eight hours to accomplish necessary software updates and other installations at least four times per year, typically in March, June, September, and December. In addition, they stated that there are "small outages" at least six times per year. Scheduled downtime is generally planned for times when the CJIS Division expects minimal customer activity (e.g., early morning hours). As shown in Table 3, IAFIS experienced scheduled downtime on a monthly basis for the six-month period that we reviewed (November 2003 through April 2004). CJIS Division officials acknowledged the frequent downtime and told us that they are working to limit scheduled downtime to the expected four times per year, but that it is "not one of their highest priorities." They stated that the CJIS Division is currently researching methods of installing software faster to reduce scheduled downtime from eight hours to approximately one hour, and is considering including a "hot maintenance concept" in the Next Generation IAFIS in which some software upgrades could be accomplished without taking the system out of service.[45]

Customer notification procedures. During IAFIS downtime, responses to DHS requests for fingerprint searches may be delayed.[46] Unscheduled delays, in particular, can present a significant problem for the Border Patrol, which relies on quick response times in order to process apprehended aliens. The CJIS Division policy is to notify customers if IAFIS cannot respond to queries within 10 minutes for the DHS, and 2 hours for other customers. However, CJIS Division officials stated that, particularly during March 2004, the CJIS Division was unable to notify the Border Patrol of the IAFIS problems

[45] Next Generation IAFIS is discussed in more detail later in this report.

[46] Delays in response time may also be due to problems at the DHS site or with other FBI systems.

in a timely manner. The CJIS Division later provided the DHS with written explanations of the problems, but a Border Patrol senior agent told us that he was frustrated by the extended IAFIS downtime (specifically during March), lengthy repair time, and an inability to directly contact the CJIS Division help desk.

To improve customer notification, on May 5, 2004, the CJIS Division modified the "call tree" that it uses to notify IAFIS users (and other CJIS Division system customers) of unscheduled downtime and other system problems to include the DHS help desk. In addition, the CJIS Division now sends a message to a designated individual at the US-VISIT Program Management Office, who then notifies locally designated area coordinators of the downtime via e-mail. The US-VISIT Program Management Office confirmed to us that it is now receiving better notice of such outages.

Lack of backup increases risk of service loss. In addition to causing downtime when components are out of service, the lack of backup systems for IAFIS means that, if a catastrophe severely damages the IAFIS system, there is no backup that can continue to provide electronic fingerprint identification services to law enforcement authorities. Copies of IAFIS data are sent to an off-site location regularly, however.[47] In February 2004, at the request of the Department, the IAFIS contractor (Lockheed Martin) prepared two reports that describe options for developing a disaster recovery site to ensure continuation of CJIS Division operations (including IAFIS, the NCIC, the National Instant Criminal Background Check System, and other services) in case of a catastrophe at the CJIS facility.[48] The reports confirm that "If the data the CJIS division maintains were destroyed, law enforcement services throughout the United States would be severely degraded." The reports recommend developing a "mirror" site that would cost an estimated $174 million and take up to eight years to complete.

Although it was not originally a requirement, CJIS officials told us, during an October 2004 follow-up interview, that the backup site is now required to ensure continual IAFIS availability during normal downtime, as well as in the event of a disaster. They also told us that the CJIS Division awarded a contract for an Enterprise Storage Area Network, which will replicate IAFIS

[47] US-VISIT and IDENT have redundant search capability with databases residing in Rockville, Maryland, and Dallas, Texas.

[48] Final Report on the Analysis of Alternative Concepts for Disaster Recovery, February 26, 2004; and Final Report on the Methodology to Plan, Design, Develop, and Implement CJIS Disaster Recovery.

data, in real-time, to an off-site location. While such a system would more effectively safeguard IAFIS data, it would not be capable of processing search requests during downtime. The CJIS Division is also considering developing an interim disaster recovery site and is evaluating the projected costs.

Although interim measures to improve border security have been implemented, the longer-term effort to achieve the fully interoperable biometric fingerprint identification system directed by Congress has stalled due to two principal issues. First, the Department, the DHS and the DOS have not agreed on a uniform Technology Standard for collecting fingerprint information. Second, the DHS disagrees with the Department that a fully interoperable system must provide federal, state, and local law enforcement agencies with ready access to IDENT and US-VISIT immigration records. Until these issues are resolved, some criminal aliens will not be identified as they try to enter the United States, illegal aliens already in the United States may not be identified, and the speed and accuracy of identification checks will be significantly reduced. In addition, the federal government may face significant costs to later re-engineer the fingerprint systems to correct deficiencies.

Interim Measures to Improve Border Security Have Been Implemented, But Efforts to Achieve the Fully Interoperable Fingerprint Biometric Identification System Directed By Congress Have Stalled.

As described in the background section of this report, since we last reported on the status of the integration project in March 2004, the Department and the DHS have implemented several interim measures to improve border security. With the implementation of US-VISIT on January 1, 2004, the DHS will now check about 43 million of the 260 million annual visitors' fingerprints against data extracted from the FBI's IAFIS. On May 17, 2004, the FBI began providing daily rather than bi-weekly Wants and Warrants electronic extracts to the DHS, as recommended in the OIG's Batres report. Also, on September 21, 2004, the DHS finished deploying Version 1.2 IDENT/IAFIS workstations to all Border Patrol stations, and is in the process of deploying integrated workstations to all United States ports of entry, to be completed by December 31, 2005.

However, even with these significant interim measures, the fully interoperable biometric fingerprint system directed by Congress has not been achieved. The current system is not a fully interoperable biometric fingerprint

system because: (1) the Department, the DHS, and the DOS have not implemented a uniform fingerprint collection methodology; and (2) law enforcement agencies still do not have direct access to all of the DHS's immigration fingerprint biometrics information. Efforts to implement a system that corrects these deficiencies have stalled because of a failure to agree on standard collection methodologies, and disagreement over the extent to which agencies will have access to each other's fingerprint data.

At the direction of Congress, the NIST developed a Technology Standard to establish a uniform method for collecting fingerprint information. In the Patriot Act, as amended by the Border Security Act, Congress directed the NIST, jointly with the Attorney General and Secretary of State, to develop and certify a technology standard for verifying the identity of those seeking a visa to visit the United States. In January 2003, the NIST, the Attorney General, and the Secretary of State submitted a joint report to Congress containing recommendations on the most effective Technology Standard for an interoperable biometric database.[49] The Technology Standard recommended by the NIST called for ten flat fingerprints to be taken for enrollment and checking of large biometric databases. The NIST further recommended that two flat fingerprints and a digital picture be used to confirm the identity of a person against his or her own existing record, but not for enrollment.

The NIST continued to conduct research on fingerprint biometrics throughout 2003 and 2004, and issued several subsequent reports. In these reports, the NIST analyzed the fingerprint matching performance and accuracy of: (1) IAFIS, using flat and rolled prints and two or more fingers;[50] (2) US-VISIT, using flat prints and one-to-one identify verification; and (3) fingerprint vendor technology, using operational fingerprint data from a variety of United States government sources. Regarding enrollment speed, the NIST found that taking ten flat fingerprints took 10 to 15 seconds longer than taking two flat fingerprints, using current fingerprint scanning technology.[51] Regarding the effects on response time, the NIST confirmed other research that found that providing more fingerprints substantially speeds search processing by increasing the filtering of the database (which reduces the number of fingerprints actually searched). The NIST also found that search accuracy

[49] *Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Document*, January 2003.

[50] Taking more than two but less than ten flat fingerprints was an option considered, including taking eight flat fingerprints (not using the thumbprints).

[51] The NIST found that two flat fingerprints can be taken in approximately 10-15 seconds, and that ten flat fingerprints can be taken in approximately 30 seconds.

increased (i.e., there were fewer false positives) when the maximum number of fingers (ten) was used to search a database.[52] This was true for all the fingerprint matching systems that the NIST tested. In September 2004, the NIST provided Congress with a summary of its recommendations for a fingerprint Technology Standard. The summary reported that the extensive testing of biometric systems conducted by the NIST in 2003 and 2004 confirmed the NIST's January 2003 recommended Technology Standard of ten flat fingerprints for enrollment and two flat fingerprints and a digital picture for identity verification.

The Department, the DHS and the DOS Have Not Agreed on a Uniform Technology Standard for Collecting Fingerprint Information.

The Department, the DHS, and the DOS have not agreed to begin collecting fingerprint biometric information in a uniform manner. At present, the Department standard is to collect ten rolled fingerprints for enrollment in IAFIS, although the Department also accepts that two flat fingerprints may be used to subsequently verify aliens' identities by checking their fingerprints against their own records (one-to-one matches). The DHS collects two flat fingerprints at ports of entry to enroll visitors into US-VISIT. The DHS also collects ten rolled fingerprints from apprehended aliens at Border Patrol stations and from visitors referred to secondary inspection at ports of entry that are not going to be admitted to the United States to check IAFIS, but enrolls them in IDENT using only two fingerprints. If an officer decides to book an apprehended alien, an officer transmits ten rolled fingerprints to IAFIS and to the Biometrics Support Center to enroll the alien in the lookout database. At United States consulates, the DOS collects two flat fingerprints to enroll individuals applying for visas into US-VISIT. Each of the departments' positions regarding implementation of a fingerprint collection standard is discussed below.

The Department position on collecting fingerprint information. The Department endorsed the recommendations in the NIST's Technology Standard. All Department officials we spoke with stated that direct queries of the criminal and immigration databases using ten flat fingerprints (instead of two) would enable more complete and rapid adjudication of individuals seeking

[52] The false positive rate, or false accept rate, is the probability that the system will incorrectly determine that a search fingerprint and a file fingerprint are matches. This would occur if a traveler is mistakenly matched as a criminal hit. The false negative rate, or false reject rate, is the probability that the system will not identify a search fingerprint match when the match is in the system. This would occur if a criminal with a record in IAFIS is not identified when his or her fingerprints are searched.

admission to the United States. They also stated that taking ten flat fingerprints would reduce the number of false positives, and offer more options for system design and interoperability across the DHS, the DOS, the Department, and other agencies. A ten flat fingerprint system would also significantly increase the probability of making a match on latent fingerprints from crime scenes.

Department officials stated that acting promptly to implement a system to collect ten flat fingerprints could reduce system upgrade costs, minimize the volume of re-enrollments, and reduce the inconvenience to foreign travelers. Finally, although the Department officials stated that all systems should collect ten flat fingerprints, they also stated that the systems must be flexible so that upgrades in biometric capture technology, such as the ability to collect ten rolled fingerprints quickly and accurately, could be incorporated in the future.

Consistent with the above, the Department has stated that it believes that the US-VISIT fingerprint workstations at consulates and ports of entry should be modified to collect ten flat prints for enrollment in the database. Because the NIST found that ten flat fingerprints could be taken in almost the same time as the two flat prints, the Department believes this option could be implemented within one year. In its draft proposal to the Policy Coordination Committee, the Department's estimate was that it would cost the Department $103 million in the first year to implement a ten-flat fingerprint system.[53]

The DHS position on fingerprint collection. Although not a party to the original NIST study, the DHS officials we spoke with were aware of the NIST Technology Standard and DHS staff participated in the discussions that led to the publication of the NIST Technology Standard. In April 2004, we asked the US-VISIT Deputy Director whether, and when, the DHS would begin taking more than two fingerprints to enroll individuals in US-VISIT. He responded that the DHS plans to continue with the current two-print process, and will make a decision regarding eight or ten prints "based on recommendations by the NIST and as the technology evolves," as it is still "an open question" whether the DHS is required to collect more than two fingerprints for US-VISIT. The DHS officials continue to maintain this position. However, in the DHS's May 28, 2004, Statement of Work, which described the scope of the Prime Contractor's obligations under the contract to develop US-VISIT, the DHS stated that a move to taking eight fingerprints at consular offices worldwide is

[53] The Department also estimated first year costs for the DOS's visa processing to be $13.3 million, and $59 million for the DHS. DOS officials said that its cost estimates for moving to a 10-fingerprint system are higher than suggested by the DOJ, but the DOS officials did not provide a cost estimate.

"in planning." Also, on July 18, 2003, the Homeland Security Council Deputies approved the use of a photograph and two fingerprints for initial US-VISIT deployment in sea and air ports of entry. At the same time, the Deputies directed the DHS and the DOS to work with the Homeland Security Council and the Office of Management and Budget to develop future plans to migrate to an eight fingerprint system.

The DHS officials also stated that operationally IAFIS cannot meet the rapid response time of 15 to 20 seconds that is needed when visitors are checked against the US-VISIT watch list at primary inspection.[54] DHS officials also said they would have to purchase more expensive scanners and reconfigure the primary inspection work space to accommodate the scanners.

The DOS position on fingerprint collection. DOS officials told us that DOS consulates are taking two flat fingerprints of visa applicants because this meets the congressional mandate to implement standardized fingerprint collection at all consulate posts no later than October 26, 2004.[55] Regarding the possibility of implementing an eight or ten print system, the Deputy Assistant Secretary of State for Visa Services told us that the DOS will be guided "by what the scientists [i.e., the NIST] say." She acknowledged the NIST's finding that too many false positives could occur with a two-print system, and stated that, at the point that the system began returning an unacceptable number of false positives, the DOS would go to a system using more than two fingerprints. The Deputy Assistant Secretary and other DOS officials cited the following concerns associated with implementing a fingerprint system that uses more than two fingerprints:

- Cost and resource issues. DOS officials told us that they have resisted going to more than two prints largely because the scanners used to take

[54] Although the rapid response time is essential at the primary inspection booths, it is much less an issue for secondary inspection and for the consular posts where more time can be taken before deciding whether to admit a visitor into the United States or grant a visa.

[55] The Border Security Act, Section 303 (b)(1) states, "not later than October 26, 2004, the Attorney General and the Secretary of State shall issue to aliens only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers. The Attorney General and the Secretary of State shall jointly establish document authentication standards and biometric identifiers standards to be employed on such visas and other travel and entry documents from among those biometric identifiers recognized by domestic and international standards organizations." Although the deadline has been extended one year, the DOS officials stated that all visa-issuing consulates would be transmitting two fingerprints to the DHS to be checked against the US-VISIT watch list by October 26, 2004.

ten fingerprints are more expensive and staff would have to be retrained to use the new equipment.

- Need for visa applicants to remain in clear view. Because DOS employees at consulates must operate behind a "hard line" (a glass window separating visa applicants from employees), they must have a clear view of visa applicants to verify that individuals are physically placing their own fingers on the scanner. Fingerprint scanners that are too large to mount on the window ledge may have to be placed where there can be no clear view of visa applicants and could make it difficult for non-English-speaking applicants to understand how to scan their fingerprints. As a result, the ten-print scanners may have to be installed off-site, which would be inefficient for visa processing.

- Ten-prints viewed as criminal. DOS officials told us that the two-print system has been well received by visa applicants thus far. However, the officials expressed concern that visa applicants may view the requirement to provide ten fingerprints as a criminal booking procedure, which the DOS is concerned could discourage travel to the United States.

Table 4 (next page) provides a comparison of the fingerprint collection methods used by the Department, the DHS, and the DOS and the pros and cons of each method.

TABLE 4 - COMPARISON OF FINGERPRINT COLLECTION METHODS			
Methods	Used By	Pros	Cons
Rolled prints of 10 fingers (10-rolled prints)	DOJ: Used as the IAFIS Criminal Master File enrollment standard DHS: Used to check apprehended aliens against IAFIS Criminal Master File; used to enroll aliens in the IDENT Lookout database; used to enroll aliens to be booked in IAFIS Criminal Master File (CAR booking); used for background checks prior to issuing lawful permanent resident card or granting citizenship. DOS: Not used	Provides the most complete information for identifying individuals Search accuracy; results in among the fewest false positive hits Provide the most information to match against latent fingerprints Greatest categorization of fingerprints reduces search to about 2 percent of database, enabling the most efficient use of processing power	Taking 10 rolled prints is time consuming and labor intensive Most difficult to take prints of acceptable quality (highest enroll reject rate) Requires different/more expensive equipment Most intrusive (operator must physically roll subjects' fingers) Most objectionable to foreign visitors
Flat-pressed prints of 10 fingers (10-flat prints)	DOJ: FBI is currently implementing this as the standard for civil enrollments and conducting background checks DHS: Not used DOS: Not used NIST recommended standard to enroll and search interoperable systems	Search accuracy for identifying criminals in IAFIS is statistically indistinguishable from using 10-rolled prints Takes only 10 to 15 seconds longer than taking 2-flat prints Less intrusive than 10-rolled prints – operator need not touch subject Fewer false positives than 2-prints Improved categorization of fingerprints reduces search to about 6 percent of database, enabling more efficient use of processing power	More expensive than two flats Perceived as more intrusive than two flats Slower IAFIS searches than 10 rolled Provides less information than 10-prints for identifying latent fingerprints
Flat-pressed prints of 2 fingers (2-flat prints)	DOJ: Not used, but accepted for one-to-one verification matches DHS: used to enroll aliens in IDENT apprehension database as well as for later searches of this database; used to enroll visitors at ports of entry in the US-VISIT database (if not done by DOS) DOS: used at consulates to search US-VISIT watch list database and enroll visa applicants in US-VISIT NIST recommended standard for one-to-one verifications only	Least expensive for equipment and labor Least intrusive for subjects Least objectionable for foreign visitors Acceptable search time when used to check 2-print databases Fastest and easiest to take prints of acceptable quality (lowest enroll reject rate)	Least accurate, results in most false positive hits and more false frequent negatives (i.e., missed identification of criminal on file) Least categorization makes it inefficient for searching 10-print databases, such as IAFIS (requires searching 70 percent of database) Provides least information for identifying latent fingerprints, which may be from any of 10 fingers Possibility of finger sequence errors

The DHS Disagrees with the Department that a Fully Interoperable System Must Provide Federal, State, and Local Law Enforcement Agencies with Ready Access to IDENT and US-VISIT Immigration Records.

The second barrier to further progress on implementing an IDENT/IAFIS system that is fully interoperable, including with US-VISIT, is that the DHS has not agreed to provide the Department and other law enforcement agencies with direct access to US-VISIT records. In the Border Security Act, Congress directed creation of "an interoperable electronic data system to provide current and immediate access to information databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or determine the admissibility or deportability of an alien."[56] Both the Border Security and Patriot Acts further specified that information in the system be "readily and easily accessible" to immigration officials and law enforcement or intelligence officers responsible for investigating or identifying aliens.[57]

On June 22, 2004, the Homeland Security Council Deputies stated that the Department and the FBI should provide a proposal with suggested language to provide the FBI with access to US-VISIT. On August 3, the Deputies stated that by August 6, 2004, the DHS will provide the FBI with 100 accounts for accessing US-VISIT data or, if this is not possible, define the way forward to overcome the technical or other obstacles impeding this access.

In October 2004, the DHS drafted an MOU to grant user accounts to 30 individuals named by the FBI for accessing US-VISIT.[58] On November 1, 2004, the DHS sent a memorandum to the Deputy Director of the Homeland Security Council stating that it had met its obligations to provide the FBI with full access to its US-VISIT records. In the memorandum, the DHS stated that it had provided training on the data limitations of US-VISIT records to these 30 individuals. In the memorandum, the DHS also stated that it would provide US-VISIT access and training to an additional 200 users whom the FBI indicated also need access to US-VISIT. However, Department officials told us

[56] Enhanced Border Security and Visa Reform Act of 2002 (P.L. 107-173), Section 202(a)(2).

[57] The Border Security Act specifies federal law enforcement, whereas the Patriot Act includes all law enforcement officers. See Enhanced Border Security and Visa Reform Act of 2002 (P.L. 107-173), Section 202(a)(5) and USA PATRIOT Act (P.L. 107-56), Section 403(c)(3).

[58] In its November 1, 2004, memorandum to the Homeland Security Council, the DHS stated that the MOU is currently being circulated for review and clearance with the Department and the FBI.

that they are disappointed at the slow pace and limited scope of the access that the DHS has provided thus far and do not consider that the FBI has "full and immediate" access to the US-VISIT database.

Further, little progress has been made toward providing the DHS's apprehension and criminal history information to other federal, state, and local law enforcement agencies. We found that the DHS's current plans do not ensure that the information in the DHS's IDENT and US-VISIT databases will be "readily and easily accessible" to the Department or other federal, state, and local law enforcement agencies. Progress to interoperability has been stymied by disagreements over how it is to be achieved. Each of the Departments' positions on this issue is discussed below.

The Department's position on law enforcement access to immigration data. According to Department of Justice officials we spoke with, a fully interoperable system should provide direct, real-time access to data from the IDENT, IAFIS, and US-VISIT databases to other federal and local law enforcement agencies. In the Department's submission to the OMB working group supporting the Homeland Security Council Deputies, JMD defined interoperability as:

> The seamless ability to share data that is complete, accurate current, and timely (available as needed) among and between participating stakeholders. The flow of information being shared must be multi-directional, not just one-way.

The need for multi-directional sharing was echoed by Department officials we spoke with. For example, on June 15, 2004, we interviewed a Section Chief at the CJIS Division who stated that the FBI's primary issue with the current process of the FBI sending the DHS extracts from IAFIS is the lack of direct access to DHS information. The Section Chief explained that the FBI supports collecting and sharing biometric information; however, the information sharing should be a "two-way street" – that is, the DHS must also share its information with the FBI. For investigations and special queries, the Section Chief stated that the FBI must be able to search any United States government database directly, including IDENT, in a timely manner.

Information in the IDENT database, specifically the alerts in the apprehensions file, is not in the IAFIS database. Alerts flag the records of aliens who did not meet the criteria for inclusion in the lookout database but nevertheless who should be closely scrutinized or detained if apprehended. Alerts include warnings about aliens who may present threats to officer safety. This information would be useful to federal, state, and local law enforcement officers who might encounter the aliens. If the FBI is unable to directly access

the information in IDENT and US-VISIT, it will be less able to identify aliens arrested in the United States who have violated their immigration status, tell employers the status of an applicant for a sensitive position, and coordinate with the DOS to ensure that law enforcement can identify persons of interest when they apply for a visa.

We asked whether the FBI's position had been communicated to the DHS, and the FBI Section Chief told us that at every opportunity during frequent meetings with representatives from the DHS he reiterates the FBI's need for direct access to the DHS databases. The Section Chief said he even has asked DHS representatives directly *when* the FBI will have access to DHS data, but has received no response. Further, CJIS Division executives we interviewed confirmed the FBI's need for multi-directional interoperability.

In another interview, a Senior Information Technology Specialist in the CJIS Division's Operations Branch confirmed the Department's position on interoperability and law enforcement access to DHS data. He told us that interoperability for the FBI means that law enforcement personnel must have access to information about previously apprehended individuals who have again illegally entered the United States. He explained that the most valuable aspect of interoperability is that all the DHS and FBI data would be available to law enforcement personnel the way that CAR transactions are currently available to anyone who queries IAFIS.

Further, Department officials stated that an interoperable environment should reduce or eliminate the replication of records in multiple databases. The "principles of interoperability" that the Department submitted to the Homeland Security Council Deputies stated: "Providing large data extracts from one system to another is the antithesis of interoperability." FBI officials also stated that sending the DHS extracts of IAFIS data (e.g., Wants and Warrants) is an inefficient and untimely practice. The CJIS Division Section Chief mentioned above told us that the FBI would prefer that the DHS search IAFIS directly, as do other users. However, the Section Chief explained that the DHS does not want to directly search IAFIS and wants the FBI to continue sending DHS extracts so that the DHS can build its own database of duplicate information. He also stated that providing extracts to the DHS is not efficient or cost-effective for the FBI as it requires human intervention to move the records to compact disks and send them to the DHS.

Finally, Department officials stated that non-citizens have minimal rights under the Privacy Act. Although the DHS made the policy decision to afford US-VISIT enrollees privacy protections, these protections do not preclude the sharing of information for law enforcement purposes.

The DHS position on law enforcement access to immigration data. The DHS officials we spoke with did not agree with the Department's vision of interoperability. In our interviews with DHS officials, they stated that law enforcement officials outside of the DHS should not have access to US-VISIT records because of privacy concerns. They also cautioned that the law enforcement records on individuals in the IDENT database are not the individual's comprehensive immigration records. In addition, they stated IDENT may have outdated or incomplete information. While outdated or incomplete data does not compromise the utility of the database, DHS officials said that it may result in errors if relied on by other law enforcement agencies.

Privacy concerns with access to US-VISIT data. Regarding US-VISIT, Program Managers from the DHS's US-VISIT Program Management Office told us that they view US-VISIT as wholly separate from IDENT/IAFIS. They explained that the fingerprint records stored in US-VISIT are from people who are presumed innocent and that US-VISIT is considered a "benefit" or "good guys" database. Conversely, IDENT and ENFORCE are on the enforcement side and are considered "bad guys" databases, as they are comprised primarily of immigration violators. The US-VISIT Deputy Director told us that the DHS is particularly concerned about guarding the data in US-VISIT to protect the privacy of visiting foreign nationals who are presumed to be non-criminals. The DHS has extended the principles and protections of the 1974 Privacy Act to all individuals processed through US-VISIT and include a process for redress if an individual has a complaint. The US-VISIT Program Office worked closely with the DHS Privacy Officer to develop the US-VISIT privacy policy. The policy explains who the program affects, what information is collected, how the information is used, and how people can find out what information is retained.

DHS Program Managers stated that another issue is ownership of US-VISIT records. The US-VISIT Deputy Director believed strongly that the DHS has the ability to store, and can "maintain the integrity of, foreign nationals' fingerprints." Regarding access by other law enforcement agencies, he stated that records in the database can be searched for law enforcement purposes on a case-by-case basis. He reiterated, though, that the FBI should not be given the authority to search the database directly. Instead, the DHS can check the US-VISIT fingerprints against a criminal watch list or for other agencies if the FBI or any other law enforcement agency has a "legitimate reason" to query the records.

The US-VISIT Deputy Director and the US-VISIT Program Managers told us that law enforcement personnel can get access to immigration data by submitting a search request for a "subject of interest" to the DHS, the Law Enforcement Support Center, or the Biometrics Support Center. For example, the Virginia State Police have expressed interest in having access to law

enforcement immigration information on aliens they encounter. The Program Managers explained that if during a traffic stop an officer finds a subject of interest, the officer could contact the Law Enforcement Support Center, which maintains updated records on immigration violators and is capable of placing a "detainer" on a deported felon. We asked when such information would be available more immediately via direct access. The US-VISIT Deputy Director stated that the DHS's prime contractor, Accenture, is responsible for defining the interoperability scheme for working with local law enforcement.[59] That is, in conjunction with DHS officials, Accenture must help decide how best to provide federal, state and local law enforcement with access to IDENT data.

IDENT does not reflect updated immigration status. The US-VISIT Program Managers also told us that the IDENT and US-VISIT databases cannot be relied upon to accurately determine immigration status because immigration status is dynamic. The databases were created to serve different purposes and populations and may not contain current and complete immigration data. For example, if an individual is apprehended along the border and naturalized two years later, IDENT would contain information on the apprehension but may not contain information on the subsequent naturalization. The latter information is kept in other databases that are available to immigration officers, but not to law enforcement agencies querying IDENT. This is important, the Program Managers stated, because it creates the potential for police officers using incomplete information to apprehend someone that they think is an immigration violator. According to the US-VISIT Program Managers, there have not yet been any detailed discussions about how to resolve this issue.

In addition to disagreeing with the Department that other law enforcement agencies should be able to directly access US-VISIT, DHS officials also disagree that the current practice of extracting records from IAFIS to IDENT fails to meet the requirement for integrating the systems. The DHS officials told us that they believe they have already achieved an acceptably integrated IDENT/IAFIS system by having access to the Department's data in IAFIS through the FBI's now-daily transmission of its Wants and Warrants file, and the monthly transmission of suspected terrorists' and military detainees' fingerprints on a compact disk.

Similarly, the DHS has stated this same position to Congress. During an April 1, 2004, hearing before the Immigration and Border Security Subcommittee of the Senate Judiciary Subcommittee, Senator Chambliss asked the DHS Assistant Secretary for Border and Transportation Security

[59] At the time of this interview, the DHS had not yet awarded the contract. The contract was awarded to Accenture on June 2, 2004.

Policy and Planning whether the DHS agreed with a recommendation in the OIG's March 2004 report that the Department should develop and implement an MOU with the DHS to guide integration of IDENT and IAFIS. The Assistant Secretary indicated that he disagreed with the recommendation because "…we have an integrated system…that can be used by the Border Patrol to essentially query both the IDENT system, which has a record of people that have been illegally deported or denied entry and so forth, as well as the IAFIS system, which is the FBI's huge fingerprint database of people with criminal records. So,…we have an integrated system."

The DOS position on law enforcement access to immigration data. DOS officials told us that, in their opinion, the FBI should have access to certain DHS data, such as entry and exit information in US-VISIT. They told us that during interagency meetings they have encouraged the DHS to share this information with the FBI, but they recognize the DHS's privacy concerns. The DOS offered to share its textual visa applicant information with the FBI and plans to sign an MOU with the FBI regarding procedures for sharing such information. Information from visa applicants is stored in the Consular Consolidated Database, which does not contain fingerprint data, only photographs and textual information on applicants. DOS officials explained that, under the MOU, certain CJIS Division representatives would have access to the Consular Consolidated Database. The DOS officials believed that direct FBI access to the DOS Consular Consolidated Database will be a significant improvement over past procedures when the FBI relied on the DOS Security Advisory Opinions.

Although the DOS supports FBI access to US-VISIT data, it does not support taking ten flat fingerprints from visa applicants to query IAFIS directly. Instead, the DOS supports the current process of the FBI providing extracts of its IAFIS data to the DHS. The DOS suggested that the FBI transfer all foreign-born criminal history data in IAFIS to IDENT. During a June 23, 2004, interview with DOS officials, we explained that the Department considers that as an interim measure until long-term interoperability and direct access was achieved. However, the Deputy Assistant Secretary of State for Visa Services told us that the current process of FBI transferring information from IAFIS to IDENT is "the way to go," and believes that "it's working." She responded that the DOS does *not* consider this to be only an interim measure. She also stated that the DOS should maintain the fingerprints its officers enroll at the consular posts because this would best ensure the integrity of the fingerprints collected overseas and allow them to verify that an individual provided his or her own fingerprints.

The Department disagrees with the DHS's and the DOS's positions on interoperability and access to immigration biometrics records in IDENT and

US-VISIT. The Department's position is that a fully interoperable system should provide direct, real-time, multi-directional sharing of data with other federal, state, and local law enforcement agencies. Currently, no direct connection between IAFIS and IDENT or US-VISIT makes this possible. The Department maintains that the interim measure of providing large extracts of IAFIS data to DHS, while valuable in the short-term, is time-consuming and inefficient. Most important, it does not ensure the most complete and timely identification of criminal aliens and known or suspected terrorists.

We also found that the Attorney General and the CIO have communicated the Department's position on interoperability to the DHS on several occasions. On November 6, 2003, the Attorney General wrote a letter to DHS Secretary Ridge, citing the need for increased coordination between the Department and the DHS.[60] The Attorney General's letter also included a letter, dated September 8, 2003, from the Department's CIO to the DHS's CIO that proposed a broad MOU between the Department and the DHS that would cover policy and business processes related to US-VISIT, interoperability of IAFIS with US-VISIT, identity enrollment and the NIST standard, information sharing between US-VISIT and federal, state and local law enforcement, and the role of IDENT/IAFIS in the US-VISIT strategy and schedule, including upgrading integrated workstations.

On May 25, 2004, the Attorney General sent a memorandum to the Homeland Security Council representatives, including the Deputy Secretary of DHS and the Secretary of State, to reiterate the Department's position on interoperability as it relates to US-VISIT. The Attorney General stated that the two principles of safety and security for Americans and a quick and accurate processing of people should guide the US-VISIT program. Regarding safety and security, the Attorney General stated:

> . . . the best way to protect our safety and security is to make our various fingerprint systems fully interoperable. This will maximize our ability to apprehend or exclude potential terrorists and other violent criminals. . . While this will require additional resources, I believe that . . . it is better to spend those funds developing the proper system now. The alternative of continuing to rely on separate systems and extracts and deciding later that we need interoperability would entail substantial delays and even more expense. I believe that DHS, DOJ/FBI, and State should move towards this goal as quickly as possible.

[60] On January 27, 2004, the Attorney General re-sent the November 6, 2003, letter to Secretary Ridge, because the Secretary did not receive the original letter.

Regarding the quick and accurate processing of people, the Attorney General stated:

> We need to implement technology and establish a fingerprint standard that minimizes the "false positive" problem…Large numbers of "false positives" could severely slow down and/or compromise our inspection processes and have adverse security, foreign policy and commercial consequences. . . it is my view that we need to rely on our best scientists to determine the specific standard we should adopt for fingerprint enrollment to accomplish this…I believe that this will result in an enrollment standard of more than two fingerprints.

Until These Issues are Resolved, Risks Remain that Criminal Aliens Will Not Be Identified as They Try to Enter the United States, Illegal Aliens May Not Be Identified, and the Speed and Accuracy of Identification Checks Will Be Significantly Reduced.

The majority of visitors to the United States are still not checked against the most complete and current law enforcement records to identify criminal aliens. The IAFIS Criminal Master File contains over 47 million fingerprint records. As of September 2004, the FBI has copied many of the IAFIS records most likely to be associated with aliens and provided them to the DHS for inclusion in IDENT (see text box, next page). However, the records provided through September 2004 amount to only one percent or less of all IAFIS records.

Under the current US-VISIT system, the vast majority of the 118,000 daily visitors will be checked against the records copied into IDENT [using two fingerprints]. Because the US-VISIT, IAFIS, and IDENT systems are not interoperable, only a select number of visitors who are subjected to additional screening are checked against the full Criminal Master File in IAFIS. Current DHS estimates indicate that the DHS plans to conduct a full check on only about 800 visitors a day (about 0.7 percent of all visitors entering the United States). However, a draft August 2004 report by JMD demonstrates that not checking aliens against the full IAFIS database increases the risk of admitting criminal aliens.[61]

[61] "Cost and Operational Effectiveness Analysis, Second Report to Congress," August 27, 2004, Justice Management Division, Management and Planning Staff, United States Department of Justice.

JMD's Metrics study report. [62] In an August 2004 draft Metrics report, JMD reported that querying individuals directly against IAFIS resulted in a significant increase in the number of criminals identified, and that failing to conduct IAFIS queries leaves the United States vulnerable to criminal aliens and terrorists entering the country undetected. In this study, JMD analyzed 179,094 encounters with aliens that occurred during 2003 at 40 sites (21 Border Patrol stations and 19 ports of entry) using Version 1.2 IDENT/IAFIS workstations. Of the encounters examined, 164,232 occurred at Border Patrol sites and 14,862 occurred at ports of entry. As described in the Background Section, the Version 1.2 workstations enable the DHS to query IAFIS directly (in addition to IDENT). The Metrics study examined whether searching IAFIS, as opposed to searching only IDENT, resulted in the identification of more criminals seeking entry into the United States. The study also identified the most serious offenses the criminals had committed.

IAFIS Records Copied Into IDENT

Latent Fingerprints. Approximately 7,000 latent fingerprints collected at crime scenes, and approximately 250 latent fingerprints related to known or suspected terrorist activity.

Known or Suspected Terrorist Fingerprints. Approximately 15,000 fingerprints of known or suspected terrorists, including military detainees being held oversees, updated monthly.

Wants and Warrants. A daily list of about 141,000 records of active warrants for individuals with an unknown or foreign birthplace or prior arrest on immigration charges. The DHS electronically scans the list to identify new and deleted records, and requests fingerprint images that it does not have.

Criminals from High Risk Countries. About 179,500 fingerprint records of males from 25 countries, such as Iraq, Iran, Syria, and the Sudan, designated as high risk (a one-time effort).

All Potential Foreign Criminals. At the DHS's request, the FBI identified about 7 million records that list foreign or no place of birth or a prior arrest on immigration charges. These records are being extracted and added to the IDENT database, but because the FBI limits the DHS to 3,000 IRQs per day, at the current rate it will take over 6 years to fully extract these fingerprint records.*

***NOTE:** Because IDENT may not have the capacity to hold all 7 million records, the DHS is currently trying to prioritize the most serious criminal offenders.

Sex Offenders. About 11,000 fingerprint records of convicted sex offenders who have an unknown or foreign birthplace, or prior arrest on immigration charges.

The Metrics study found that, of the 179,094 aliens checked, 80,150 (44.8 percent) had no record, and 74,924 (41.8 percent) had prior administrative immigration violations. The remaining 24,020 (13.4 percent) of the aliens had criminal records (20,346 from Border Patrol stations and 3,674 from ports of entry). Importantly, the study found that at least 17,553 of these criminal aliens – 73.1 percent – were identified *only as a result of the IAFIS*

[62] This is the second of several expected Metrics reports and it updates the first report of July 18, 2003.

Table 5: Criminal Hits Attributed to IAFIS by Most Serious Offense		
Most Serious Offense	**Hits**	**Percent of Total**
Immigration	3,526	28.6%
Dangerous Drugs	1,851	15.0%
Assault	1,574	12.8%
Weapons Offenses	180	1.5%
Robbery	128	1.0%
Sexual Assault	116	0.9%
Sex Offenses	84	0.7%
Kidnapping	41	0.3%
Homicide	38	0.3%
All Others	4,794	38.9%
Total	**12,332**	**100.0%**

Source: JMD Metrics Report

query. Almost three quarters of the criminal aliens attempting to enter the country would not have been identified as criminals by IDENT alone because immigration officials would not have had access to their criminal records in IAFIS.

Many of the criminal aliens had committed serious violations. JMD analyzed the criminal rap sheets of 12,332 of the 17,553 individuals identified by IAFIS to determine the nature and severity of their criminal histories. The most serious offense on 7,538 (61 percent) of the rap sheets fell into one of nine categories identified as "special interest" because they would likely result in action by a United States Attorney or the Executive Office of Immigration Review (Table 5, next page). Many had committed crimes that raised public safety or border security concerns. Nearly one-third (4,012) committed violent crimes or were involved with dangerous drugs. Also, many were repeat offenders. Over half the rap sheets contained multiple charges and 15.6 percent had five or more charges while 4.4 percent had 10 or more charges.

The JMD Assistant Director for Management and Planning told us that JMD would like to conduct a study of US-VISIT fingerprint data similar to the Metrics Study described above. In conjunction with a statistician, the CJIS Division, the DHS, and JMD could take statistically valid random samples of US-VISIT data from various ports of entry and from other relevant immigration biometric databases used for enforcement or benefit purposes in IDENT and search the DHS's two-flat fingerprint data against IAFIS. The objective of the study would be to assess the risk of not checking the fingerprints of all visitors subject to US-VISIT or those exempt from US-VISIT against the complete IAFIS database. The research would be conducted so as not to disrupt normal IAFIS operations. Officials from JMD have discussed this possible study with the

DHS, but the DHS and JMD have not yet agreed on the parameters of the study or on the data that is to be sampled.

Until a standard ten fingerprint methodology is adopted and an interoperable system is implemented, the speed and accuracy of identification checks will be significantly reduced. Research conducted by MitreTek showed that taking more fingerprint impressions greatly speeds fingerprint searches.[63] When IAFIS processes a fingerprint search, it first classifies the fingerprints according to pattern (e.g., left loop, right loop, whorl, and arch). It then conducts a fingerprint matching check against only records of fingerprints having the same basic patterns. For searches using ten rolled fingerprints, about 98 percent of the database can be filtered out so that the fingerprint matching is conducted on only about 2 percent of the records. Using ten flat prints allows about 94 percent of the database to be filtered out. In contrast, with two flat fingerprints about 70 percent of the database must be matched, increasing the amount of processing required by about 35 fold over ten rolled prints. These research findings strongly suggest that, because the US-VISIT system is not collecting fingerprints in accordance with the NIST's recommended Technology Standard, response times will be delayed as the US-VISIT database grows. In addition to longer processing times, using fewer than ten fingerprints results in reduced accuracy and a greater likelihood of identifying false positives.

Further, the Metrics study report found that the data extracts from IAFIS to IDENT are prone to error because, for example, one of the selection criteria relies upon self-reported data (e.g., place of birth). However, aliens being arrested have an incentive to lie about their nationality to avoid deportation. Also, many United States citizens have an unknown or foreign place of birth. The result is that the records of United States citizens may be loaded into the IDENT database, while the records of some non-United States citizens and potential criminal aliens are not included. The Metrics study found that the Wants and Warrants extract failed to include 22 percent (121 of 541) of criminal aliens with active Wants and Warrants.[64]

[63] Implications of the IDENT IAFIS Image Quality Study for Visa Fingerprint Processing, MitreTek Systems, October 31, 2002.

[64] Of the 22 percent (121) of the criminal aliens with outstanding Wants and Warrants who were not included in the extracts, 14 percent (77) were not included because they did not meet the extract criteria (foreign or no place of birth, prior immigration violation) and 8 percent (44) may have been missed due to the two-week lag time between extracts.

The Federal Government May Face Significant Costs to Later Re-engineer the Different Fingerprint Systems

According to Department officials, if timely action is not taken to adopt a uniform fingerprint methodology, such as the NIST Technology Standard, and establish the parameters for an interoperable system, the costs to re-engineer the systems later will be significantly greater. Further, enrollment records currently being created in US-VISIT may be incompatible with the Technology Standard that ultimately is adopted. In that case, individuals may have to be re-enrolled in order for their records to be complete. Among the decisions that must be made are: Who should be subjected to fingerprint searches? What fingerprint collection standard should be used? Which databases are to be queried? Who will have access to the information in each database? How will the information be used? Who will maintain the databases?

The need for resolution of these questions is increasing because the Department is proceeding with the development of new systems. For example, JMD had begun planning for Version 2 of IDENT/IAFIS and the FBI is planning for the Next Generation IAFIS. Further, in June 2004 the Department submitted a draft proposal to members of the Policy Coordination Committee containing options, costing up to $280 million, for a long-term strategy to achieve interoperability.[65] The Department recognized the potential for future costs, stating:

> Significant cost savings will also be achieved by avoiding mistakes now that will be costly in the future. By collecting [more than two fingerprints] for US-VISIT enrollment now instead of later, system upgrade costs will be lower and the volume of re-enrollments will be minimized to reduce the inconvenience to foreign travelers.

Because of the disagreements about collection of uniform biometric fingerprint information and the extent to which systems should be made interoperable, the Department, the DHS, and the DOS still have not developed an MOU on how law enforcement agencies will be given direct access to all of the DHS's immigration data.

[65] Policy Coordination Committee Concept Paper Proposal: Law Enforcement Interoperability with US-VISIT and Overseas Visa Issuance, June 2004 draft.

In response to our March 2004 report on *IDENT/IAFIS: The Batres Case and the Status of the Integration Project*, the Department, the CJIS Division, and the DHS have taken action to address four of the five recommendations. The Department assigned responsibility for the integration project within the Department to its CIO, the development of a fully integrated IDENT/IAFIS is being expeditiously pursued, Wants and Warrants updates are now provided to the DHS on a daily basis, and the criminal histories of aliens who have IAFIS hits are made available to Border Patrol agents and immigration inspectors. However, the Department and the DHS still have not developed a Memorandum of Understanding to guide the future efforts to integrate the IDENT and IAFIS systems.

No Memorandum of Understanding developed. In our March 2004 report, we recommended that the Department work with the DHS to develop and implement an MOU to guide integration of IAFIS and IDENT. The Conference Report accompanying the FY 2004 omnibus appropriations legislation also directed the Department to develop an MOU with the DHS and other appropriate federal agencies regarding the continued integration of fingerprint systems.

Yet, as described above, the Department, the DHS, and the DOS have not developed and implemented the MOU because of fundamental disagreements over what the attributes of an interoperable biometric fingerprint system should be, or the extent to which systems should be made interoperable. Although the Department, the DHS, and the DOS have continued to work together in interagency working groups to discuss operational and technical problems of mutual concern, high-level decisions regarding the fundamental issues must be resolved before agreement can be reached on the long-term interoperability of the IAFIS, IDENT, and US-VISIT systems.

Responsibility for the integration project within the Department has been assigned to the CIO. We recommended that the Department assign responsibility for coordinating and overseeing the integration project to a senior Department official. The Department assigned that responsibility for coordinating the integration project to the Department CIO.

The development of a fully integrated IDENT/IAFIS is being expeditiously pursued. We recommended that the Department and the DHS pursue expeditiously the development of an integrated version of IDENT/IAFIS that would provide the DHS apprehension and criminal history information to other federal, state, and local law enforcement agencies. We found that the Department CIO, JMD, and the FBI's CJIS Division have taken several actions that will promote the implementation of an interoperable IDENT/IAFIS system. Examples of these actions are:

Long-term interoperability solutions developed. The CIO stated that the Department would do whatever is necessary to improve the situation in the short-term, but that it is important to focus on the long-term vision so that the necessary planning can be done. The CIO and JMD developed and submitted to the Policy Coordination Committee two options for a long-term solution to implement a biometric fingerprint system that will effectively meet the security and law enforcement needs of all concerned parties. Both options assume that up to 42 million foreign visitors a year will be searched directly against IAFIS records and that the FBI will have law enforcement access to US-VISIT files. The options also entail modifying existing equipment to take more than two flat fingerprints at consulates and at ports of entry. Under the first option, termed the "unified approach," the FBI CJIS Division in West Virginia would become the consolidated U.S. Government center for biometric expertise, providing a single source for enrollment, retention, criminal history, and terrorist data.

The CJIS Division would maintain and administer the DHS biometrics databases, including the IDENT lookout and apprehension databases and US-VISIT data, and would provide a dedicated, partitioned AFIS for US-VISIT. The DHS would continue to own its data and set relevant privacy and operating rules to govern its use through MOUs with the CJIS Division. The second option, termed the "enhanced status quo," described a solution in which modified IDENT/IAFIS workstations could be deployed at the visa-issuing consulates and embassies and at primary US-VISIT enrollment stations at the ports of entry to allow the capture of more than two flat fingerprints in order to thoroughly evaluate visitors before they arrive, and to reduce false positives and false negatives.

The DoD has begun establishing the consolidated service center model described in the Department's option one. The DoD is implementing the same type of dedicated, partitioned AFIS that the FBI would provide for US-VISIT data, and has already begun building the system. The DoD, like the DHS, has privacy concerns with its fingerprint data. In addition, the DoD has taken action to ensure that all the fingerprints it collects from military detainees and known and suspected terrorists are interoperable with IAFIS. On February 2, 2004, the DoD's CIO announced a new requirement for all existing DoD

fingerprint collection systems to be upgraded to become interoperable with IAFIS by December 31, 2004.

Fast Capture technology. On September 4, 2004, the Department, through the National Institute of Justice, issued a solicitation due by November 8, 2004, for fast capture fingerprint/palm print technology. The goal "is to fund the development and demonstration of technology that will quickly capture ten rolled-equivalent fingerprints and/or palm prints; significantly improve the fingerprint and palm print image quality over current technologies; reduce the failure to enroll rate (due to poor quality) over current technologies; and be affordable, rugged, portable, relatively unobtrusive in size and deployable in the near future."

Planned IDENT/IAFIS modifications to track immigration violators in IAFIS. In the Department's FY 2005 Budget Request, JMD requested $5 million to start work on making immigration information accessible to other federal, state and local law enforcement agencies, as directed by Congress. If approved, JMD plans to begin designing a modification to IDENT/IAFIS Version 2 to create an Immigration Violator File that will include apprehension data from IDENT and new enrollees submitted by the DHS.[66]

The FBI has begun planning for "Next Generation IAFIS." We found that the CJIS Division has started developing concepts for Next Generation IAFIS, and has prepared a FY 2006 budget request and justification covering the projected implementation costs. The CJIS Division has requested over $77 million in FY 2006 for Next Generation IAFIS initiatives, which are intended to:

- *Improve fingerprint identification accuracy:* The IAFIS uses technology that is almost 10 years old, and the original AFIS specifications required only 95 percent accuracy.[67] The latest biometric technologies now offer advances in filtering, feature extraction, and matching algorithms that provide accuracy rates of up to 99.9 percent.

- *Allow flat fingerprint searching capability and increased search capacity.* The CJIS Division must implement flat fingerprint capability for IAFIS to

[66] IDENT/IAFIS OMB Circular A-11, Exhibit 300, FY 2005. This was planned before US-VISIT and may no longer be applicable. Progress has stalled and JMD is not actively pursuing this approach as it awaits further decisions.

[67] These are likely to be false negatives (IAFIS may not return the correct identification decision even if the match is in the IAFIS database).

process flat fingerprints for background checks for employment and licensing, and for ten-print and latent searches. The budget request estimates that increases in these searches "could easily triple current workloads" and proposes that the IAFIS ten-print search capacity be expanded to accommodate 200,000 searches per day, plus up to 1,000 latent searches per day.

- *Create an Enhanced Terrorist Identification Service.* This proposed specialized biometrics database will contain real-time fingerprint data from known and suspected terrorists and wanted persons. Enhanced Terrorist Identification Service will allow submissions of less than ten fingerprint images and will provide a response within seconds that will reflect a status of "no record" or "warning."

- *Implement a "zone" concept.* Next Generation IAFIS will enhance the civil fingerprint functionality to allow for the exchange of records between four databases or "zones," one of which will support the Enhanced Terrorist Identification Service database. The zone concept will provide a means for ensuring segregation of DHS US-VISIT records.

The FBI is implementing standard processing for ten flat fingerprints. In April 2004, the CJIS Division published a study with the NIST, the Secret Service, and the states of Ohio, Texas, and New York that examined the feasibility of a "national, rapid, and positive fingerprint-based identification background check system for authorized non-criminal justice [civil] purposes."[68] The study analyzed the feasibility of processing fingerprint searches using ten flat, rather than ten rolled, fingerprints through IAFIS and found them comparable to civil fingerprint checks. The results are directly applicable to the handling of US-VISIT fingerprint queries should US-VISIT begin taking ten flat fingerprints. Based on review of a CJIS report, the Compact Council provisionally approved the report's 6-month implementation option for ten-flat fingerprints, and the CJIS Advisory Policy Board subsequently endorsed the Compact Council's decision.[69] The Council approved the recommendation to accept ten flat fingerprints so long as the reliability meets or exceeds the IAFIS specifications, the FBI identifies a

[68] National Fingerprint-Based Applicant Check Study (N-FACS), FBI CJIS Division, April 5, 2004, p. iii.

[69] The Compact Council is a 15-member group that governs the use of criminal history records maintained by the CJIS Division for non-criminal justice (civil) purposes, per the FBI's National Crime Prevention and Privacy Compact. The Compact Council advises the CJIS Advisory Policy Board on civil fingerprint standards.

standard for flat capture devices, and there is no degradation to current IAFIS criminal justice services.

Wants and Warrants updates are now provided to the DHS on a daily basis. We recommended that the Department work with the DHS to update IDENT with FBI information on a daily, rather than bi-weekly, basis. Working together with DHS on an accelerated schedule, the CJIS Division began to provide daily Wants and Warrants extracts from IAFIS to the DHS on May 17, 2004.

Criminal histories of aliens who have IAFIS hits are made available to Border Patrol agents. We recommended that the Department coordinate with the DHS to establish procedures to ensure that the criminal histories of all aliens who have a lookout or IAFIS hit are provided to and reviewed by the Border Patrol. As part of the DHS expedited deployment, the CBP established and issued written procedures that outlined appropriate steps for handling lookout hits and that ensured that criminal histories of all aliens who have a lookout or IAFIS hit are provided to and reviewed by the Border Patrol.

CONCLUSION AND RECOMMENDATIONS

Although significant positive steps have been taken to expedite the deployment of the initial integrated version of IDENT/IAFIS, progress toward the longer term goal of making biometric fingerprint systems fully interoperable has stalled. Under the current process, the FBI extracts certain data from IAFIS and provides it to the DHS for insertion into IDENT. The result is an unnecessary duplication of data, and the use of some erroneous, untimely, and incomplete data by the DHS in lieu of direct queries of the most current and complete information contained in IAFIS. Further, because only a small percentage of aliens at ports of entry are being searched against IAFIS, the likelihood of missing a criminal alien or terrorist is increased.

The FBI and other law enforcement agencies (federal, state, and local) have no access to the DHS's IDENT and US-VISIT immigration records, particularly the alerts in the apprehensions file, which are not in the IAFIS database. Among other things, these alerts flag the records of aliens who did not meet the criteria for inclusion in the lookout database but nevertheless who should be closely scrutinized or detained if apprehended. If the FBI is unable to directly access the information in IDENT and US-VISIT, it will be less able to identify aliens arrested in the United States who have violated their immigration status, tell employers the status of an applicant for a sensitive position, and coordinate with the DOS to ensure that law enforcement can identify persons of interest when they apply for a visa.

Critical differences continue to exist between federal agencies over the fundamental method of capturing fingerprint information. The NIST-recommended Technology Standard calls for using ten flat fingerprints to implement a long-term interoperable biometric fingerprint system. However, the DHS and the DOS have neither agreed to implement the uniform fingerprint Technology Standard recommended by the NIST nor agreed how to develop a fully interoperable system that provides law enforcement agencies with "readily and easily accessible" access to IDENT and US-VISIT immigration records as required by Congress in both the Patriot and Border Security Acts. Because these capabilities have not been developed, over 99 percent of the visitors seeking admission to the United States will only be checked against the US-VISIT watch list. Because that watch list relies on a limited number of records extracted from the IAFIS Criminal Master File, the checks will not be as complete as those made directly against the full 47-million record IAFIS Criminal Master File. As the Department's Metrics Study showed, when only extracts are checked, many criminal aliens – including many who committed violent crimes that threaten public safety – are not identified and may be unknowingly admitted to the United States.

For the Department to effectively proceed with planning to make IAFIS interoperable with the biometric fingerprint systems of the DHS and the DOS, high-level policy decisions must be made regarding who should be subjected to fingerprint searches, the fingerprint collection standard to be used, the databases to be queried, who will have access to the information, how the information will be used, and who will maintain the databases. We recommend that the Department seek to have the federal government address those decisions in a timely and coordinated manner. We therefore recommend that the Department:

1. Within 90 days of the enactment of the Department's FY 2005 appropriations act, report to the Homeland Security Council and Congress that the Department, the DHS, and the DOS have reached an impasse and cannot complete the MOU directed by Congress. The report should formally request that the Homeland Security Council or Congress decide on the adoption of the NIST Technology Standard and define the capabilities to be provided in the interoperable system;

2. Increase the transmission of the fingerprints of Known or Suspected Terrorists from the FBI to the DHS from monthly to at least weekly;

3. Request access to a random sample of data from US-VISIT and other relevant immigration biometric databases used for enforcement or benefit purposes for comparison to IAFIS in order to determine the risk posed by not checking all visitors against IAFIS;

4. Coordinate with the DHS to identify the capacity needed to conduct IAFIS searches on all visitors referred to secondary inspection and inform the Department's CIO how the capacity of IAFIS (now planned to be 20,000 searches by October 1, 2005) could be increased to handle that level of activity;

5. Develop options for the eventual upgrade of IAFIS to enable the system to conduct ten flat fingerprint searches on all US-VISIT enrollees and TPRS submissions from the Border Patrol and from the ports of entry; and

6. Take steps to ensure that IAFIS meets its availability requirement of 99 percent.

APPENDIX I
BACKGROUND ON FBI AND INS AUTOMATED FINGERPRINT IDENTIFICATION DATABASES

United States immigration authorities have long recognized the need for an automated fingerprint identification system to quickly determine the immigration and criminal histories of aliens apprehended at or near the border. More than one million aliens are apprehended each year attempting to enter the United States illegally. Many of these aliens are apprehended in large groups, and the Border Patrol lacks the resources to detain them for extended periods of time. Consequently, the vast majority are voluntarily returned to their country of origin, mostly to Mexico, without any criminal charges being filed.

Immigration authorities need to be able to quickly determine which of these aliens should be detained for prosecution based on multiple illegal entries, reentering the United States after a prior deportation, alien smuggling, a current arrest warrant, or a criminal record. Historically, in order to identify which individuals to detain for possible prosecution or deportation, the INS had to rely on the names provided by the apprehended aliens and check them against its databases or other paper records. This method was ineffective because aliens often used false or different names. Also, many aliens have similar names, and spelling errors result in problems identifying individuals accurately.

Automated Biometric Identification System (IDENT)

In 1989, Congress provided the initial funding for the INS to develop an automated fingerprint identification system that eventually became known as IDENT. While one of the main purposes of IDENT was to identify and prosecute repeat immigration offenders, another significant purpose was to identify criminal aliens who should be detained. The 1989 conference report described Congress's rationale for funding the project:

> Illegal immigration continues at alarming rates, and criminal alien statistics provided by the INS indicate that a growing proportion of aliens are drug smugglers, known criminals, and suspected terrorists. Emerging technology in the area of automated fingerprint identification systems has the potential for providing empirical data to clearly define the problem of recidivism as well as immediately identify those criminal

aliens who should remain in the custody of the INS (emphasis added).[70]

Integrated Automated Fingerprint Identification System (IAFIS)

At about the same time, the FBI began to overhaul its paper-based fingerprint card system, which it had maintained since the 1920s, to create a new automated fingerprint identification system that would allow electronic searches for fingerprint matches. Since the 1920s the FBI's Identification Division has maintained a central repository of ten-prints of criminal offenders' fingerprints. In 1967, the FBI created the National Crime Information Center (NCIC) to provide a national database of computerized information on individuals with active Wants and Warrants, stolen articles, vehicles, guns, license plates, and other data. Fingerprint information for wanted and missing persons is submitted by participating federal, state, and local law enforcement agencies, of which over 80,000 have access to NCIC. In February 1990, the NCIC Advisory Policy Board recommended that the FBI update its paper-based fingerprint identification system and create a new automated system, which eventually became known as the FBI's IAFIS. IAFIS currently contains in its Criminal Master File over 47 million ten-print criminal fingerprint records that can be electronically compared against submitted fingerprints. During 1990 and 1991, the INS and FBI met to discuss possible coordination of their planned automated fingerprint identification systems. They discussed how the FBI's IAFIS and the INS's proposed system could be linked to ensure uniform high-quality fingerprint image and electronic transmission standards for fingerprints and identification data so that they could be transmitted among different fingerprint identification systems.

From the start, the INS and the FBI recognized that integration of their separate automated fingerprint identification systems would benefit both agencies. An integrated system would reduce the likelihood that INS would release an alien who had a serious criminal record and prior deportations. It also would enable federal, state, and local law enforcement authorities to search latent fingerprints against an immigration database of illegal border crossers, especially if ten rolled fingerprints were taken.

[70] See H.R. Conf. Rep. No. 100-979 at 30, accompanying H.R. 4728, 100th CONG., 2d SESS. (1988).

III. IMPLEMENTATION OF SEPARATE FBI AND INS DATABASES

Two versus Ten Fingerprints

An early difference of opinion between the INS and the FBI was whether the INS should take two fingerprints or ten fingerprints from the aliens it apprehended. The FBI, along with state and local law enforcement agencies, believed that the INS should take ten rolled fingerprints so that they could be matched against ten-fingerprint records in the law enforcement databases or any latent fingerprints obtained at crime scenes. Because fingerprints at crime scenes may be from any finger, the long-established law enforcement standard requires that officers take fingerprints from all ten fingers.

The INS emphasized that a fast response time was critical because the INS could not detain large numbers of apprehended aliens for long periods of time while waiting for responses to criminal checks. The INS believed that taking ten fingerprints of all apprehended aliens would take too long and would adversely affect its ability to carry out its mission.

Between 1991 and 1993, the INS operated a pilot Automated Fingerprint Identification System (AFIS) project in the San Diego Border Patrol Sector. In 1994, Congress allocated funding for the INS's automated system. During an April 1994 meeting regarding the deployment of IDENT, the FBI told the INS that without additional development time and money, the FBI's planned IAFIS system could not meet the INS's need to handle a high volume of fingerprints (for more than one million aliens apprehended annually), and provide the quick response time (two minutes or less) for each encounter. Further, the FBI said that the alternative of searching and matching the two fingerprints captured by IDENT against the FBI's planned IAFIS ten-fingerprint database would require much more computer power than the FBI had in order to provide the response time that the INS needed.

Therefore, in 1994 the INS decided to move forward with implementation of its separate IDENT system, independent from the FBI's IAFIS system. In order to meet its own needs, the FBI decided that its automated fingerprint system, IAFIS, would contain all ten fingerprints and provide a response in two hours for high priority electronic requests and a longer time for lower priority and non-electronic requests.

The Border Patrol's Use of IDENT

The INS's IDENT system was designed to automatically alert personnel at the Western Identification Network Automated Fingerprint Identification Center (WIN/AFIS) whenever IDENT returned a lookout hit indicating an outstanding

warrant for an apprehended alien.[71] INS procedures required WIN/AFIS personnel promptly telephone the apprehending Border Patrol personnel to confirm the lookout match and to inform the Border Patrol agents of the nature of the warrant and the contact numbers for the appropriate law enforcement officials regarding the warrant. This contact generally occurs within one hour. A Border Patrol supervisor then contacts law enforcement officials who issued the warrant to determine whether they want to pay for and transport the alien to their jurisdiction for prosecution.

Typically, if the issuing authorities do not want the alien transported, and there is no other reason to detain the alien, the Border Patrol voluntarily returns the alien across the border. However, some circumstances warrant further detention and investigation. For example, if a processing agent learns – usually from the alien himself, or through prior IDENT entries from previous apprehensions – that the alien has a prior criminal history, the Border Patrol may seek the prosecution of the alien for the offense of Entry Without Inspection.[72] Also, if the agent learns that the alien has a prior deportation, the law requires reinstatement of the prior order of deportation, and the alien is not eligible for voluntary return to Mexico.[73] Upon learning of the prior deportation, the processing agent should confirm the alien's prior criminal history.

Moreover, an alien likely will be prosecuted for the felony charge of Reentry After Deportation if the alien has a record of a prior felony or aggravated felony. A conviction for Reentry After Deportation carries a potential sentence of up to 10 years' imprisonment for an alien with a prior criminal record of a felony or three misdemeanors, or a sentence of up to 20 years' imprisonment for an alien with a prior aggravated felony conviction pursuant to § 1326(b).

---

[71] Formed in 1989, WIN/AFIS contains information from state and federal criminal justice agencies in seven Western states. Its database contains about 2.5 million arrest records from those member states and from the INS. Its fingerprint search capabilities are provided by a large-scale AFIS installation in Sacramento, California. An additional unit called the INS WIN/AFIS Service Center provided technical support to INS facilities performing criminal searches on WIN and handled WIN registrations. The INS WIN/AFIS Service Center operates 7 days per week, 24 hours per day, and is staffed by contract employees who were qualified fingerprint examiners and who could make fingerprint matches.

[72] While the Border Patrol technically could bring this charge for every illegal entry, it is not feasible to bring charges on each apprehended alien because of the effect on prosecutorial, judicial, and detention resources.

[73] See 8 USC § 1231(a)(5).

The agents at Border Patrol stations that do not have direct access to the FBI's criminal records must telephone the Border Patrol sector's communications office, commonly known as the "radio room," which has direct links to various criminal and immigration databases. These databases include the FBI's NCIC; immigration databases containing records of prior immigration contacts with the alien, such as deportations; and a DHS database, the Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS), which is typically used by inspectors at ports of entry to check incoming travelers.

Because the Border Patrol lacks the manpower to conduct separate criminal and immigration history checks for every apprehended alien, these additional database checks are requested for only the small fraction of the apprehended aliens whose behavior, appearances, outstanding warrants, or other information in IDENT raises concerns with the Border Patrol agents processing the aliens.

JMD's Fingerprint Database Integration Efforts

In the mid-1990's, the Attorney General established a Fingerprint Coordination Working Group, which included representatives from the INS and the FBI, to address problems in fingerprint procedures. As part of this effort, the Department's Justice Management Division (JMD) reviewed integration issues of the INS and FBI automated fingerprint identification systems, and attempted to coordinate the integration of their separate systems.

In March 1998, the OIG issued a report evaluating the INS's implementation of IDENT.[74] The OIG found that the INS was enrolling less than two-thirds of the aliens apprehended along the U.S.-Mexico border into the IDENT system. In addition, the INS was entering into the IDENT lookout database the fingerprints of only 41 percent of the aliens deported and denied admission into the United States in FY 1996. Of these aliens, only 24 percent had accompanying photographs entered into IDENT, even though the INS relied on photographs as an important method of confirming identification. The OIG found virtually no controls in place to ensure the quality of data entered into the IDENT lookout database, which resulted in duplicate records and invalid data. The OIG report also raised concerns that the INS had not provided sufficient training to its employees on the use of IDENT, and that these failures hampered the INS's ability to make consistent and effective use of IDENT.

[74] See "Review of the Immigration and Naturalization Service's Automated Biometric Identification System," March 1998.

Two months later, in May 1998, in response to a letter from Congressman Alan Mollohan urging that consideration be given to integrating the IDENT and IAFIS systems, JMD issued a report recommending that the INS retain IDENT to meet INS internal requirements, but that the INS adopt ten-printing as a long-term policy goal. The JMD report concluded that, properly funded, this option would permit the Border Patrol to maintain processing times while providing other law enforcement agencies with a fingerprint database that could be searched. The report also recommended a 12-month pilot study, to begin in the fall of 1999, of a ten-fingerprint system in selected Border Patrol stations.

IV. THE RESENDEZ CASE

In 1999, the consequences of INS's inability to identify criminal aliens without integrated IAFIS and IDENT databases were illustrated tragically by the case of Rafael Resendez-Ramirez (Resendez).[75] In 1998, the Border Patrol in Texas and New Mexico apprehended Resendez, a Mexican citizen with an extensive criminal record, seven times while crossing the border illegally. Each time he was voluntarily returned to Mexico.

Unbeknownst to the agents who apprehended and voluntarily returned Resendez in accord with normal Border Patrol policy, Resendez had an extensive criminal history in the United States. He had been convicted previously on at least eight separate occasions for crimes that included aggravated felonies. Resendez also had been previously deported to Mexico at least three times and voluntarily returned to Mexico by the INS at least four times.

During each of the seven apprehensions in 1998, the Border Patrol agents who processed Resendez through IDENT did not learn of his criminal record or past deportations. Because IDENT was not integrated with IAFIS, and because IDENT only included information about apprehended aliens on a day-forward basis, IDENT did not contain any information about Resendez's past convictions and deportations. Also, because Resendez had been apprehended less than the threshold number of times for prosecution for Entry Without Inspection, the Border Patrol agents simply enrolled Resendez in IDENT on each of these encounters and voluntarily returned him to Mexico. They were not required to check, and did not check, FBI databases for criminal history information and outstanding warrants on him.

[75] The facts of the Resendez case are detailed in a March 2000 OIG report entitled, "The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of Its IDENT Automated Fingerprint Identification System."

In early 1999, evidence linked Resendez to several brutal murders in Texas and Kentucky, and warrants were issued for his arrest. Other federal and local law enforcement authorities contacted INS personnel at least four times to discuss the warrants and the evidence against Resendez, and to ensure that the INS placed a lookout for Resendez in the event that he was apprehended again while illegally entering the country. Yet, none of the INS investigators who were contacted by the law enforcement officers thought to have a lookout placed for Resendez in IDENT based on the warrants, either because the INS investigators were unfamiliar with IDENT, or because they thought it was the job of others to enter the warrants.

On June 1, 1999 – at the same time that state and federal warrants for Resendez were outstanding and law enforcement officers were searching for Resendez in connection with several murders – Border Patrol agents in Santa Teresa, New Mexico, apprehended Resendez again crossing the border illegally. They processed him in IDENT according to their standard practice. IDENT identified Resendez as a recidivist border crosser, but nothing in IDENT alerted the Border Patrol agents that he was wanted for murder by the FBI and local law enforcement authorities. Nor did IDENT disclose Resendez's extensive criminal history. Therefore, the Border Patrol did not detain Resendez and, following its standard policy, voluntarily returned him to Mexico. Within days, Resendez illegally returned to the United States and committed four more murders.

In mid-June 1999, a Border Patrol Intelligence Officer in Texas enrolled Resendez into the IDENT lookout database to ensure that he would be detained if encountered again by the INS. At that time, the Border Patrol discovered that its agents had recently released Resendez despite the outstanding warrant for his arrest for murder. Finally, On July 13, 1999, Resendez surrendered to U.S. law enforcement authorities and on May 18, 2000, he was convicted of capital murder and sentenced to death.

V. RENEWED EMPHASIS ON INTEGRATION OF IDENT AND IAFIS

In July 1999, a House Committee on Appropriations report, with the Resendez incident clearly in mind, stated:

> [T]he Committee continues to be concerned about the inadequacies of this system [IDENT], specifically with regard to its ability to identify wanted criminals who may be apprehended by INS Border Patrol agents and inspectors along the border…the Committee repeatedly raised concerns that the IDENT database was not integrated with FBI's IAFIS database.

Law Enforcement Access to INS Data

The House Report expressed the belief that federal, state, and local law enforcement should have access to INS fingerprint information and that the INS should have the full benefit of FBI criminal history records. The House report directed the INS to suspend further deployment of IDENT until the Department submitted to the House Appropriations committee a plan for integration of IDENT and IAFIS. The Conference Report for the Department's FY 2000 appropriations included this provision.

JMD Assigned to Coordinate Integration

In response to the Congressional directive, the Department assigned JMD to coordinate the efforts to develop an integration plan. On August 12, 1999, JMD convened a "Fingerprint Summit" meeting, attended by representatives of the FBI and INS, to discuss a plan for integrating IDENT and IAFIS. The conceptual model agreed to at that meeting required that the INS be able to check fingerprints of apprehended aliens against all fingerprint records in IAFIS and that federal, state, and local law enforcement agencies be able to access the INS's fingerprint records through IAFIS.

JMD issues integration report. On March 1, 2000, JMD's Management Planning Staff issued a report entitled "Implementation Plan for Integrating the INS' IDENT and the FBI's IAFIS Fingerprint Data." The report stated that, "The INS and FBI have acknowledged that integrating IDENT with IAFIS would greatly benefit both agencies, as well as federal, state, and local law enforcement." The report further stated that such integration:

> has the potential to: reduce the likelihood that a wanted individual would be released from the INS' custody; provide federal, state, and local law enforcement an integrated picture of the criminal activity known by agencies in DOJ, including the INS histories of illegal border crossers; and enable federal, state, and local law enforcement to search latent prints against additional illegal border crossers, especially if ten-prints are taken.

The report discussed various options for integration, but directed that before any recommendation would be finalized, the INS, the FBI, and JMD would conduct three studies:

> (1) a criminality study that would estimate the percentage of apprehended illegal aliens who had been charged with more serious crimes;

(2) an engineering study that would produce a cost analysis for the integration, including alternative query response times; and

(3) an operational impact study that would assess the effect that such changes as taking ten prints would have on operations and procedures at the border.

OIG Issues Resendez Report

Also in March 2000, the OIG issued its report on the Resendez case.[76] The OIG report noted that integration of IDENT and IAFIS would provide what the IDENT lookout database did not – a check of all apprehended aliens to determine whether they have serious criminal records, prior orders of deportation, or any outstanding arrest warrants. The report recommended that the Department and its components should aggressively and expeditiously link the FBI and INS automated fingerprint systems.

The Department Conducts Three Integration Studies

From June 2000 through July 2001, the Department conducted the three studies in support of the integration project. First, the Operational Impact Study concluded that it might be feasible for the INS to take ten rolled fingerprints in many locations and check them against the FBI's IAFIS files if the INS could receive a response from the FBI within 10 minutes, except for high volume workload periods. Second, the Engineering/System Development Study concluded that IAFIS could not be searched using the IDENT two-fingerprint system in the volume and within the response time that the INS required. This study proposed an alternative approach requiring the INS to collect ten rolled fingerprints (in addition to continuing to separately take two fingerprints for IDENT). Third, the Criminality Study (based on a sample of the recidivist database) projected that a total of 136,000 (8.5 percent) of the approximately 1.6 million aliens apprehended each year by the Border Patrol and allowed instead to voluntarily depart would be detained if their fingerprints were matched against IAFIS and their criminal histories were checked.

JMD Announces Incremental Deployment of IDENT/IAFIS

In January 2001, JMD issued its FY 2002 budget request, which stated that incremental versions of the IDENT/IAFIS database would be deployed in FY 2001, with a fully integrated version deployed in FYs 2006-7. The JMD

[76] "The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of Its IDENT Automated Fingerprint Identification System."

plan called for deployment during FY 2001 of Version 1, a single ten-fingerprint workstation capable of querying IDENT using index fingerprints and IAFIS using ten fingerprints. The electronic IAFIS response would indicate a match or no match. When there was a match, IAFIS would electronically transmit the criminal rap sheet to the workstation from which the query was made.

JMD revises its plan. However, in August 2001 JMD revised its plan to slow the pace of the integration project because of concerns about operational issues relating to the Department's ability to handle the additional workload and the costs of detaining criminal aliens as projected by the criminality study. JMD also sought the delay to further study the additional workload and costs and to monitor developing biometric technologies to ensure that the Department did not commit large sums of money to an integration plan that would not take advantage of future technological advances. As a result of this revised plan, JMD reduced its original FY 2002 budget request for the integration project from $38 million to $9 million.[77] Also, the anticipated time frame for completing the first integrated version was delayed one year – from December 2001 until December 2002.

USA Patriot Act Enacted

In October 2001, in the wake of the September 11 terrorist attacks on the United States, Congress enacted the USA PATRIOT Act of 2001, Public Law 107-56 (the Patriot Act). The Patriot Act directed the expedited implementation of an integrated entry/exit data system, including the use of biometric technology.[78] The Patriot Act also required that the FBI share with the INS wanted-persons information in IAFIS to determine whether an applicant for admission at a port of entry has a criminal record. Finally, the Patriot Act required that the Department report to Congress on enhancing IAFIS and other identification systems to better identify aliens who may be wanted before their entry to or exit from the United States.[79] Subsequent Department responses to Congress regarding the Patriot Act indicated that an integrated IDENT/IAFIS was to be an integral tool to identify terrorist or criminal aliens attempting to enter the United States.

[77] The $38 million included $10 million for IDENT system operation and maintenance costs, but no funds for increased operational costs for the INS.

[78] The Data Management Improvement Act of 2000 directed the implementation of an integrated entry/exit data system (US-VISIT) and assigned deadlines for completion of the system.

[79] As of January 2004, the FBI's CJIS Division had not completed the Attorney General's report.

Wants and Warrants Records Added to IDENT

The selected input of FBI criminal records into the IDENT database over the past few years has illustrated the large number of criminal aliens who are regularly apprehended by the Border Patrol. The Wants and Warrants were added to IDENT in August 2001. From December 2001 to April 2003, 152,000 FBI Wants and Warrants fingerprint records were entered into IDENT. From January 2002 to April 2003, immigration authorities apprehended 4,820 aliens who were wanted for criminal offenses based on these records. Fifty of these aliens were wanted in connection with murder. During the same period, an additional 179,500 IAFIS criminal history fingerprint records of aliens from countries believed to be a threat to the United States were entered into IDENT and immigration personnel have matched these criminal records to 3,440 apprehended aliens.

OIG Issues Follow-up Report

In December 2001, the OIG issued another follow-up report examining the status of the continuing efforts to integrate IDENT and IAFIS.[80] The report concluded that the Department had moved slowly toward integrating the two fingerprint systems. As of December 2001, JMD's plans for the deployment of the final version of the integrated database had been delayed another year (for a total of 2 years). The OIG report recommended that the Department continue to seek expeditious linkage of the FBI and INS automated fingerprint systems, and to continue to use IDENT while the integration was proceeding. The OIG report also supported the interim measure of immediately adding to the IDENT lookout database IAFIS fingerprint records for aliens with outstanding Wants and Warrants, as well as adding fingerprint records for Known or Suspected Terrorists.

OIG report found problems in IDENT's lack of integration with IAFIS. Thus, while the IDENT database is a useful tool for identifying recidivist aliens who continue to enter the United States illegally, its lack of integration with the FBI's IAFIS database results in significant problems. First, IDENT contains only a fraction of the Criminal Master File fingerprint records in the FBI IAFIS database – limited to the Wants and Warrants that the FBI and United States Marshals Service have entered into IDENT since August 2001 and the criminal history fingerprint records of aliens from certain countries believed to pose a security risk to the United States.

[80] See OIG report entitled "Status of IDENT/IAFIS Integration," December 2001.

Second, the criminal history rap sheets which would help determine which aliens warrant prosecution were not automatically transmitted to the agents. As a result, Border Patrol agents may fail to take the extra steps needed to query the alien's criminal history information or, when Border Patrol agents initiate criminal history checks, the results may not be communicated to the processing agent (either by WIN/AFIS, the radio room, or assisting agents) in an accurate or timely manner. Third, federal, state, and local law enforcement agencies have a limited ability to access IDENT fingerprint records through their systems in order to make use of the immigration records in their investigations.

In June 2003, we reported that the IDENT/IAFIS integration project had fallen at least two years behind schedule.[81] At that time, the next major project milestone was deployment of the initial integrated version of IDENT/IAFIS, Version 1.2. Originally scheduled for December 2001, that deployment experienced a series of delays while JMD studied the operational costs of the integration (called the Metrics Study) and while the INS focused on developing the National Security Entry/Exit Registration System (NSEERS).[82]

We also reported that the integration project was at risk of further delays because JMD had not developed a transition plan for continued management of the project after the INS transferred to the DHS in March 2003. Moreover, JMD had not prepared a revised schedule for completing the full integration of IDENT and IAFIS. We found that the lack of planning resulted in confusion over whether JMD or the DHS would manage the development and deployment of the integration project. We also noted the potential loss of expertise as the DHS reassigned individuals experienced in IDENT away from the stalled integration project. The delays and lack of planning we noted for the integration project were troubling because the interim enhancements made to IDENT had resulted in an impressive record of helping to identify wanted aliens.

Our June 2003 report recommended that JMD coordinate with the DHS to identify the management, deployment, and operational issues raised by the

[81] See the OIG report entitled "Status of IDENT/IAFIS Integration," June 2003.

[82] NSEERS is a national registry for nonimmigrant aliens arriving from certain countries to the United States, or aliens meeting intelligence-based criteria and identified as presenting an elevated security concern. NSEERS, which collected background, travel, and departure information and fingerprints, was the first step taken by DOJ and then DHS to comply with the congressionally mandated requirement for a comprehensive entry/exit program by 2005. Although the NSEERS Program was superseded by the US-VISIT Program, NSEERS registration continues.

INS transfer to the DHS; prepare a revised project deployment plan; and report quarterly on the progress and interim results of the Metrics Study. We concluded that as of January 2004, some progress has been made in deploying the initial integrated versions of IDENT/IAFIS, but the integration process continued to proceed slowly. IDENT Version 1.1+ workstations had been deployed to approximately 56 DHS sites, including 25 ports of entry and 31 Border Patrol stations.[83] That represents about 12 percent of all ports of entry, and about 20 percent of all Border Patrol sites.[84]

JMD Metrics Study Findings

The first Metrics Study report sent to Congress on July 18, 2003, estimated that, as a result of improved IAFIS access, the Border Patrol was able to obtain additional criminal history information that it would not have known about for between 8.8 percent and 10.3 percent of the aliens it apprehended at the Metrics sites. Preliminary Metrics data from October through December 2003, with all sites deploying Version 1.1+, suggested that access to IAFIS provided criminal history information to the Border Patrol on between 8.5 and 11.8 percent of apprehended aliens that would not have been known by searching IDENT alone. From October 1, 2003, until January 31, 2004, the Border Patrol had 9,650 criminal hits from IAFIS that, including hits for aliens wanted in connection with 13 murders.

The FBI continued to electronically update every two weeks the Wants and Warrants file that goes into the IDENT lookout database. Every month, the FBI also provides to the lookout database an updated Known and Suspected Terrorist file, which includes fingerprint records the FBI has acquired from various law enforcement and security sources. From October 2003 until January 31, 2004, the DHS received 3,034 hits on apprehended aliens from the updated Wants and Warrants file, including 399 hits for aliens wanted for violent crimes.

[83] Version 1.1+ workstations could take ten rolled fingerprints and simultaneously query the IDENT and IAFIS databases to provide a rapid response for potential matches from IAFIS in less than 10 minutes.

[84] In addition, another 56 locations (ports of entry, Border Patrol stations, and District Offices) had received the unintegrated Version 1.1.1, which required that aliens be processed twice in order to check both the IDENT lookout database and the IAFIS criminal history records.

JMD Revises Project Schedule

JMD revised the official project schedule to reflect the delays that had been incurred through September 2003. According to JMD officials, the DHS will determine the date by which Version 1.2 is deployed nationwide. The revised schedule indicates that the final version, Version 2 – which will provide the important capability for the FBI and local law enforcement agencies to access the DHS's fingerprint and criminal history databases – will not be completed before August 2008. That is more than 5 years later than Version 2 originally was scheduled to be deployed, and almost 2 years behind the original scheduled completion date for the entire integration project. However, according to JMD officials, the scope and phasing of the entire project has undergone a thorough revision. Version 2 will incorporate what was referred to as Versions 2, 3, and 4 in the original project plan.

VI. THE BATRES CASE

In 2002, another high-profile case demonstrated the urgent need for integration of IDENT and IAFIS. Like the earlier Resendez case, this case tragically illustrated the danger of requiring immigration agents at individual Border Patrol stations to decide when they should research an apprehended alien's criminal history rather than relying on an integrated database that matches an alien's fingerprints and automatically transmits a criminal history rap sheet to the Border Patrol station within 10 minutes.

The Batres report examined the case of a Mexican citizen, Victor Manual Batres, who had been detained by the Border Patrol on two occasions in January 2002 for illegally entering the United States. On each occasion, the Border Patrol returned him voluntarily to Mexico. They did this because IDENT and IAFIS were not integrated and the apprehending Border Patrol agents did not learn of Batres' extensive criminal record or past deportation. If his full history had been learned, according to Border Patrol policies he should have been detained and prosecuted. Instead, after his voluntary return to Mexico, Batres illegally reentered the United States and traveled to Oregon in September 2002 where he brutally raped two Catholic nuns, resulting in the death of one of the nuns.

The Resendez and Batres cases both demonstrated the urgent need to integrate the separate FBI and DHS fingerprint identification databases. In the Resendez case, the INS failed to provide adequate training in IDENT policies and failed to ensure adequate understanding and use of IDENT throughout the INS. As a result, Resendez's fingerprint record in IAFIS was not entered into IDENT. In the Batres case, the Batres IAFIS fingerprint record was entered

into IDENT but his criminal history rap sheet was not automatically forwarded to the immigration agents who never requested it for review.

In these two cases, had the immigration agents been made aware of the information in the FBI databases, both Batres and Resendez would have been detained and likely incarcerated instead of being voluntarily returned to Mexico, where they subsequently were able to return to the United States and commit additional crimes.

Batres Report Findings and Recommendations

In March 2004, the Office of the Inspector General issued, "IDENT/IAFIS: The Batres Case and the Status of the Integration Project." The report again found delays in the effort to integrate the IDENT and IAFIS databases. While the report found some progress in deploying an integrated version of IDENT/IAFIS, we concluded that full integration of the two systems remained years away. The report found that the current projections from the DHS were that the two systems would not be fully integrated until at least August 2008, almost two years behind the original scheduled completion date for the full project. The report also found uncertainty as to who will be responsible for the overall management of the integration project. We also found that the integration project had been slowed by the attention placed by the DHS on other technology projects, such as US-VISIT. In addition, the transfer of the INS to the DHS had caused delays in the integration project.

The OIG report made the following recommendations to assist the Department of Justice in expediting integration of IDENT/IAFIS:

- Develop and implement a memorandum of understanding (MOU) with the DHS to guide the integration of IDENT and IAFIS;[85]

- Assign responsibility for coordinating and overseeing the integration project to a senior Department official;

- Pursue expeditiously the development of the integrated version of IDENT/IAFIS which will provide the DHS apprehension and criminal history information to other federal, state, and local law enforcement agencies;

[85] The Conference Report accompanying the FY 2004 omnibus appropriations legislation directed the DOJ to develop an MOU with the DHS and other appropriate federal agencies regarding the continued integration of fingerprint systems.

- Work with the DHS to update IDENT with FBI information on a daily, rather than bi-weekly, basis; and

- Coordinate with the DHS to establish procedures to ensure that the criminal histories of all aliens who have a lookout or IAFIS hit are provided to and reviewed by the Border Patrol.

APPENDIX II
ACRONYMS USED IN THIS REPORT

BTS	Border and Transportation Security
CAR	Criminal Answer Required
CBP	Customs and Border Protection
CIO	Chief Information Officer
CIS	Bureau of Citizenship and Immigration Services
CJIS	Criminal Justice Information Services
DAD	Deputy Assistant Director
DAAG	Deputy Assistant Attorney General
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
FBI	Federal Bureau of Investigation
HSC	Homeland Security Council
IAFIS	Integrated Automated Fingerprint Identification System
ICE	Bureau of Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
III	Interstate Identification Index
IISS	Identification and Investigative Services Section
IRQ	Fingerprint Image Request

ITMS	Information Technology Management Section
JABS	Joint Automated Booking Station
JMD	Justice Management Division
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
RMU	Requirements Management Unit
TPRS	Ten-Print Rap Sheet
US-VISIT	United States Visitor Immigrant Status Indicator Technology

APPENDIX III
DEPARTMENT (JMD) COMMENTS ON THE DRAFT REPORT

U.S. Department of Justice

Washington, D.C. 20530
December 16, 2004

MEMORANDUM FOR GLENN A. FINE
Inspector General
Office of Inspector General

FROM: Paul R. Corts
Assistant Attorney General
for Administration

SUBJECT: Comments on OIG Draft Report: IDENT/IAFIS: Follow-up Review of the Status of IDENT/IAFIS Integration

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report entitled, "IDENT/IAFIS: Follow-up Review of the Status of IDENT/IAFIS Integration." I appreciate your recognition of the significant steps that have been taken to expedite the deployment of the initial version of the integrated IDENT/IAFIS workstation, providing the Department of Homeland Security (DHS) access to criminal history records maintained by the Federal Bureau of Investigation (FBI). I also appreciate your acknowledgment of the many actions the Department of Justice (DOJ) has taken to promote the implementation of an interoperable IDENT/IAFIS system.

I believe your report has fairly and effectively presented the different perspectives of the various agencies involved in the effort to achieve interoperability between the two biometric identification systems operated by DOJ and DHS. These two agencies, plus the Department of State (DOS) and the National Institute of Standards and Technology (NIST), have different sets of mission objectives, and each one has been a forceful advocate for its respective position. The Department supports full interoperability and will continue to advocate approaches that best meet the law enforcement and counter-terrorism needs of the country. DOJ and NIST have concurred on a uniform method for collecting fingerprint information with which the DHS and DOS do not agree. It is our hope that your report will help resolve many, if not all, of the outstanding issues that you have identified for resolution.

Below are comments regarding the recommendations contained in the draft report.

1. **By December 31, 2004, report to the Homeland Security Council (HSC) and Congress that the Department, the DHS, and the DOS have reached an impasse and cannot complete the Memorandum of Understanding (MOU) directed by Congress. The report should formally request that the HSC or Congress decide on the adoption of the**

NIST Technology Standard and define the capabilities to be provided in the interoperable system.

As indicated above, it is our hope that this report will help resolve the issues related to the objective of achieving interoperability between these systems. Once your report is issued in final, we will transmit it to the HSC and ask that its members address the matter. We also intend to report to Congress on the status of this project within 90 days of the enactment of the Department's FY 2005 appropriations act.

2. **Increase the transmission of the fingerprints of Known or Suspected Terrorists from the FBI to the DHS from monthly to at least weekly.**

The FBI will provide fingerprints of Known or Suspected Terrorists within one week of establishing the record within IAFIS. The FBI is also exploring opportunities to improve its processing of Known or Suspected Terrorists. Several IAFIS system changes are in development that may allow for these records to be exchanged with DHS daily.

3. **Request access to a random sample of data from the US-VISIT and other relevant immigration biometric databases used for enforcement or benefit purposes for comparison to IAFIS in order to determine the risk posed by not checking all visitors against IAFIS.**

As reported in the draft, the Department has made such a request, but an agreement on the parameters of the study has not been reached. It is our belief that an agreement can be achieved once the other, larger issues have been resolved through the HSC.

4. **Coordinate with the DHS to identify the capacity needed to conduct IAFIS searches on all visitors referred to secondary inspection and inform the Department's CIO how the capacity of IAFIS (now planned to be 20,000 searches by October 1, 2005) could be increased to handle that level of activity**.

Until such time as the issues articulated in your report are resolved, it is premature to identify specific operational requirements and the attendant system capabilities that would be needed. As soon as these issues are settled, the Department will move expeditiously to ensure that it, and its systems, can meet expectations.

5. **Develop options for the eventual upgrade of IAFIS to enable the system to conduct ten flat fingerprint searches on all US-VISIT enrollees and TPRS submissions from the Border Patrol and from the ports of entry**.

This recommendation presupposes policy decisions that have not been made. Until policy decisions are made at the HSC level, it seems inadvisable and inappropriate to spend resources

to develop detailed options for full operational implementation.. Pending policy decisions by HSC, the Department continues exploring various options informally as to ways to further and better support US-VISIT.

6. **Take steps to ensure that IAFIS meets its availability requirement of 99 percent.**

The FBI has been working to improve IAFIS availability routinely since the system went operational in July 1999. Since IAFIS began operations, the yearly system availability has increased with each year. Several initiatives are currently underway to reduce unscheduled outages by eliminating single points of failure and creating redundancy where possible. The FBI is in the process of standardizing the hardware platforms across IAFIS. This initiative, which began in 2003 and will be completed by April 2005, will provide automated recovery capabilities to support rapid restoration of services during off-nominal events.

The FBI's long term plans to reduce both scheduled and non-scheduled outages include the development of a full system disaster recovery capability. The FBI is currently defining the concept of operations as well as the system requirements that will shape this future vision. Funding as yet has not been identified, so an implementation date has not been determined.

Again, thank you for the opportunity to comment on this draft report. We look forward to the resolution of the issues identified in your report and to further progress toward improved identification capabilities for federal, state and local governments in their efforts to keep America safe and secure.

APPENDIX IV
OIG ANALYSIS OF DOJ COMMENTS

On November 19, 2004, the Office of the Inspector General (OIG) sent copies of the draft report to the Federal Bureau of Investigation (FBI) and the Department of Justice's (DOJ) Justice Management Division (JMD) with a request for written comments.[1] The Assistant Attorney General for Administration and the FBI responded to us in a consolidated memorandum dated December 16, 2004 (Appendix III). JMD and the FBI concurred with all six of our recommendations. Our analysis of their comments follows.

RECOMMENDATIONS

Recommendation 1: By December 31, 2004, report to the Homeland Security Council (HSC) and Congress that the DOJ, the DHS, and the DOS have reached an impasse and cannot complete the MOU directed by Congress. The report should formally request that the HSC or Congress decide on the adoption of the NIST Technology Standard and define the capabilities to be provided in the interoperable system.

Status: Resolved-Open.

Summary of Response. JMD stated that it hopes that our report will help resolve the issues related to the objective of achieving interoperability between IDENT and IAFIS. JMD stated that it would transmit our final report to the HSC and ask that its members address the matter. JMD also stated that it intends to report to Congress on the status of this project within 90 days of enactment of the DOJ's FY 2005 appropriations act.

OIG Analysis. We accepted and modified the date in our recommendation to reflect the Department's proposed action. We consider the recommendation resolved but open. To close the recommendation, we request that by March 31, 2005, JMD provide a copy of the report sent to the HSC. In addition, we request that JMD provide a copy of its status report to Congress when completed.

[1] We also provided copies of the draft report to the Department of Homeland Security (DHS) and the Department of State (DOS). Our analysis of the DHS's and the DOS's comments are addressed separately.

Recommendation 2: Increase the transmission of the fingerprints of Known or Suspected Terrorists from the FBI to the DHS from monthly to at least weekly.

Status: Resolved-Open.

Summary of Response. JMD stated that the FBI will provide the fingerprints of Known or Suspected Terrorists to the DHS within one week of establishing the record in IAFIS. JMD also stated that the FBI is exploring opportunities to improve its processing of Known and Suspected Terrorists and is developing several IAFIS system changes that may allow for these records to be exchanged with the DHS on a daily basis.

OIG Analysis. We consider the recommendation resolved but open. To close the recommendation, we request that by March 31, 2005, the FBI provide: (1) documentation demonstrating that the FBI began providing the DHS with the fingerprints of Known or Suspected Terrorists within one week of establishing the record in IAFIS and (2) the status of the FBI's efforts to implement the daily transmission of these fingerprint records to the DHS. Until the DHS is able to directly access IAFIS, we encourage the FBI to continue working towards the goal of providing the DHS with the most recent fingerprint records of Known or Suspected Terrorists.

Recommendation 3: Request access to a random sample of data from US-VISIT and other relevant immigration biometric databases used for enforcement or benefit purposes for comparison to IAFIS in order to determine the risk posed by not checking all visitors against IAFIS.

Status: Resolved-Open.

Summary of Response. JMD stated that although it has not yet reached agreement with the DHS on the parameters of this proposed study, JMD believes that an agreement can be achieved once other larger issues have been resolved through the HSC.

OIG Analysis. We consider the recommendation resolved but open. To close this recommendation, we request that by March 31, 2005, JMD provide documentation of the request for access to data, the DHS/DOS response, and the results of the risk analysis conducted on any data received.

Recommendation 4: Coordinate with the DHS to identify the capacity needed to conduct IAFIS searches on all visitors referred to secondary inspection and inform the DOJ's CIO how the capacity of IAFIS could be increased to handle that level of activity.

Status: Resolved-Open.

Summary of Response. JMD stated that until the issues articulated in our report are resolved, it is premature to identify specific operational requirements and the attendant system capabilities that would be needed. JMD stated that "as soon as these issues are settled, the DOJ will move expeditiously to ensure that it, and its systems, can meet expectations."

OIG Analysis. We consider the recommendation resolved but open. To close the recommendation, we request that by March 31, 2005, JMD provide documentation demonstrating that: (1) the DOJ coordinated with the DHS to resolve issues and identify the capacity needed to conduct IAFIS searches on all visitors referred to secondary inspection and (2) the DOJ's CIO was informed of how the capacity of could be increased to handle the activity that would be generated by conducting IAFIS searches on all visitors referred to secondary inspection.

Recommendation 5: Develop options for the eventual upgrade of IAFIS to enable the system to conduct ten flat fingerprint searches on all US-VISIT enrollees and TPRS submissions from the Border Patrol.[2]

Status: Resolved-Open.

Summary of Response. JMD stated that this recommendation presupposes policy decisions that have not been made. Until policy decisions are made at the HSC level, JMD stated that it seems "inadvisable and inappropriate to spend resources to develop detailed options for full operational implementation." JMD stated that pending policy decisions by the HSC, the DOJ "continues exploring various options informally as to ways to further and better support US-VISIT."

OIG Analysis. We consider the recommendation resolved but open. We accept JMD's statement that decisions by the HSC could alter the final operational implementation requirements. Thus, by March 31, 2005, please provide a copy of the HSC's final decision on IAFIS, IDENT, and US-VISIT operational requirements; or a status report on the efforts to establish the final operational requirements and a copy of the initiatives that the FBI stated that it has developed initiatives to support improving search reliability for ten flat fingerprint searches.

[2] Ten-Print Rap Sheet (TPRS) refers to the criminal history file associated with an alien's fingerprints. Border Patrol agents and inspectors at ports of entry receive a TPRS response from IAFIS if an alien's fingerprints return a potential match to fingerprints in the IAFIS database.

To close this recommendation, we request that within 90 days after the final operational requirements are established, JMD and the FBI provide the plans developed to upgrade IAFIS to meet the requirements established.

Recommendation 6: Take steps to ensure that IAFIS meets its availability requirement of 99 percent.

Status: Resolved-Open.

Summary of Response. JMD stated that the FBI has been working to improve IAFIS availability routinely since the system became operational in July 1999. JMD stated that since that time, IAFIS system availability has increased annually and the FBI has several initiatives underway to reduce unscheduled outages by eliminating single point of failure and creating redundancy where possible. JMD stated that the FBI is currently standardizing the hardware platforms across IAFIS, which it stated will provide automated recovery capabilities to support rapid restoration of services during off-nominal events (i.e., unscheduled downtime). The FBI stated that this initiative, which began in 2003, will be completed by April 2005. JMD also stated that the FBI's long-term plans to reduce scheduled and unscheduled IAFIS outages include developing a full system disaster recovery capability. JMD stated that the FBI is currently defining the concept of operations and system requirements for this capability, but because funding for the capability has not yet been identified, the FBI has not determined the implementation date.

OIG Analysis. We consider this recommendation resolved but open. To close the recommendation, we request that by June 1, 2005, the FBI provide: (1) documentation demonstrating that it has implemented initiatives to reduce unscheduled IAFIS outages; (2) the status of efforts to standardize the hardware platforms across IAFIS; and (3) the implementation date of its long-term plans for full system disaster recovery capability, including the concept of operations and system requirements. We believe the FBI should continue to improve IAFIS availability and develop initiatives to that effect.

APPENDIX V
DHS COMMENTS ON THE DRAFT REPORT

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

Homeland Security

December 3, 2004

Glenn A. Fine
Inspector General
U. S. Department of Justice
950 Pennsylvania Avenue NW, Suite 4322
Washington, D.C. 20530-0001

Dear Mr. Fine:

Thank you for the opportunity to review and comment on the draft report entitled, IDENT/IAFIS: Follow-up Review of the Status of IDENT/IAFIS Integration. Clearly we all share the goal of protecting our nation. We believe the issue of IDENT/IAFIS integration to be extremely important to the Department of Homeland Security's (DHS) primary mission to protect America's homeland and its citizens and visitors. We welcome efforts to improve the communications and data exchange between DHS and the Department of Justice (DOJ). We also agree that further communications and interoperability must continue between the several departments involved in biometrics that are cited in your working draft.

We would like to note that there are several inaccuracies and incorrect assumptions in the draft report. In addition, we would propose alternative recommendations for your consideration as to how to move forward. Our relevant comments appear in the enclosure.

Please let me know if you have any questions. You or your staff may also contact Tom Harner of US-VISIT at (202) 298-5206 for additional information.

Sincerely,

Asa Hutchinson
Under Secretary
Border and Transportation Security

Enclosure

www.dhs.gov

Comments from the Department of Homeland Security on the Department of Justice Inspector General Draft Report
IDENT/IAFIS: Follow-up Review of the Status of IDENT/IAFIS Integration

1. Requirements of the USA PATRIOT Act were fulfilled. After having reviewed all pertinent technical studies by NIST and having considered all other relevant factors such as operational constraints and implementation costs, the Homeland Security Council (HSC) Deputies Committee, including representatives from the Department of State, the Department of Justice, the Department of Homeland Security, and the National Institute of Standards and Technology (NIST) decided on July 18, 2003, to establish as the technical standard for the US-VISIT Program two index fingerprints and a photo. Through this decision by the Deputies Committee, the requirements of the USA PATRIOT Act were fulfilled. The USA PATRIOT Act did not assign to NIST the sole responsibility for setting the technology standard, as your report indicates.

   The Deputies Committee also decided that the Department of State (DOS), the Department of Homeland Security (DHS), and the Office of Management and Budget (OMB) should conduct planning for a migration to the use of eight fingerprints. That was based on concern expressed by NIST that when the US-VISIT enrollment database grows to a certain size, the result might be a large number of false positive fingerprint matches that would require the hiring of an excessive number of fingerprint examiners to review. In other words, the primary concern was one of workload relating to clearing fingerprints through the US-VISIT enrollment database. The planning to be undertaken, in the decision of the Deputies Committee, did not relate to ten fingerprints and the use of the ten-print IAFIS fingerprint system. The problem of false positives has not materialized; however, the Department of Homeland Security is conducting appropriate planning to support the move to an eight-print system when appropriate.

2. US-VISIT has been an unprecedented success. DHS and DOS have engineered the single most significant change to the visa issuance and U.S. border inspections process ever. To date, over 13 million travelers have been processed through US-VISIT, biometrically matching their identity with their visa/passport. At ports of entry over 1,500 persons have been identified off the watch list, and hundreds have been denied entry. At consular posts, over 3,500 have been identified off of the watch list assisting DOS with the adjudication of visa issuance or denial. All of this has been done without increasing wait times or impacting legitimate trade and travel, and while protecting the privacy of travelers.

3. The draft report is misleading when it states that NIST research showed that ten "flat" fingerprints can be taken almost as quickly as two flat fingerprints. This would lead one to believe that the additional 10-15 seconds required to take ten prints of 43 million visitors per year is operationally feasible. Even discounting the processing time required, the additional 10-15 seconds required for print capture would have an enormous impact. It would require a significant number of additional inspectors and consular officers as well as significant facility modifications to handle the increase in wait times. This statement shows a lack of understanding of DHS and DOS operations.

4. US-VISIT does not use the same architecture as IAFIS. The draft report is also misleading in that it incorrectly equates the Mitre study of the FBI's IAFIS system with the DHS IDENT system. The Mitre study, referred to in the draft report, analyzed the FBI architecture, which requires use of all 10 prints in order to filter the database down to a small enough size to do a comparison on the two index prints. IDENT does not use this type of filtering in its architecture. Adding 10-prints to IDENT would actually add additional time to the process because IDENT would need to make more matches, not fewer.

5. US-VISIT is not IDENT/IAFIS. The report incorrectly assumes that the US-VISIT Program has the same set of requirements as that which generated the need for IDENT/IAFIS integration. The component of IDENT that US-VISIT uses is a traveler identification system with lookout capability. It is not designed for booking criminals. The primary US-VISIT database contains the biometrics of over 10 million enrolled legitimate travelers to the United States. This is a separate from the IDENT lookout database that receives daily extracts from IAFIS.

   The original intent behind IDENT/IAFIS integration was to provide quick access to criminal history information to INS officers during the apprehension process. Future versions were to give state and local law enforcement organizations access to IDENT immigration apprehension information. The US-VISIT enrolled population is not comprised of immigration violators.

6. IAFIS, as currently architected, cannot meet DHS operational requirements. The report incorrectly assumes that the FBI's IAFIS system could be used for US-VISIT purposes; that taking 10-prints for every traveler at ports of entry and submitting these to the FBI's IAFIS would both solve most of the interoperability issues and be beneficial. This assumption is inaccurate for the following reasons:

   - Not all criminal history records are relevant to all DHS decisions. For example, our analysis has shown that only a small percentage of the information contained in the FBI database is for wanted persons or has a bearing on whether the individual will be admissible to the U.S. A U.S. officer on port-of-entry primary does not have the time, and more importantly, the need to review the vast majority of these records.

   - IAFIS' response time on a Ten Print Rap Sheet Request (TPRS) electronic query is approximately 10 minutes. This is the best response time currently available. An inspector at primary currently enjoys a response time of less than 10 seconds.

   - IAFIS does not have the capacity to handle the volumes associated with US-VISIT. Factoring in the DOS, land border, and exit, the number of transactions may reach as much as 180,000 per day, which would be nearly 10 to 20 times the current capacity of a TPRS IAFIS search.

   - IAFIS' availability is not adequate for real-time operations. Over the last six month period, IAFIS averaged two days per month of down time (planned and unplanned). Planned outages have recently been occurring almost monthly. Unscheduled outages are

a significant problem with IAFIS as well. For example, at the time of the writing of this response, IAFIS has been down numerous times for unscheduled outages – once for as long as two hours – in the last two weeks.

- IAFIS does not have any backup capability as your working draft correctly noted. IAFIS resides in a single location, with tapes stored offsite. It would be impossible to bring the system back on line in any reasonable period of time, should something happen to its primary location. US-VISIT IDENT has redundant search capability – residing in Rockville, Maryland, and Dallas, Texas, with failover capability between the two.

- The costs of moving to an FBI-based 10-print solution are significant and given FBI's current inability to respond to operational time constraints with information focused and relevant to the decision, with little benefit. Even discounting the significant cost to the FBI required to restructure the IAFIS architecture to provide the capacity to perform the transactions quickly and improve the reliability/availability, the costs to DHS are prohibitive. Capturing 10 prints would require hundreds of additional inspectors, and significant facility modifications at the ports.

The report asserts that there would be cost savings for moving immediately to a 10-print capture system. DHS believes that this assertion is erroneous and without justification. The US-VISIT IDENT system required an initial investment of $70 million with an additional operating cost of approximate $15 million per year. Although these costs are not insignificant, the cost of moving to a 10-print FBI solution would be far greater. DHS recognizes that biometric technology is constantly evolving. And although it is not technically or economically feasible to do this at this time, with advances in capture and matching technology, it may be technically feasible to move to a multi-print system in the future. However, even if it were possible, the potential huge disruption to the travel and tourism industry, due to increased processing times and cultural resistance associated with criminality, must be analyzed prior to making these significant investments.

7. The findings of the JMD criminality study cannot be extrapolated to the US-VISIT population. The report draws an incorrect comparison between results from the Justice Management Division (JMD) metrics criminality report and US-VISIT. By definition, the populations are fundamentally different. US-VISIT contains information on travelers. The individuals described in the JMD report have already been arrested by the Border Patrol. By trying to cross the border illegally, these persons have already shown a disregard for the law, and in many cases it will not be their first time. This is precisely why DHS accelerated the deployment of the fully integrated IDENT/IAFIS terminal to all Border Patrol locations.

8. The draft incorrectly cites organizational responsibility. The working draft cites the Department of Justice and Department of State under the Enhanced Border Security Act as being responsible for implementing appropriate biometric identifier standards at ports of entry and overseas posts. This is now the responsibility of DHS and DOS.

DHS has developed an alternative proposal for how to address the need for IDENT/IAFIS interoperability, especially in relation to US-VISIT. This path is designed to achieve appropriate data exchange between DOJ and DHS.

9. DHS will monitor performance. DHS and the Department of State are aware of both the capabilities and limitations of the biometric systems employed by US-VISIT. DHS / US-VISIT continues to closely monitor the IDENT system and work with the NIST with the goal of improving system performance including false positive rates, accuracy rates, and system throughput. We will move to a multi-print system at the appropriate time to improve system performance.

10. DOJ and FBI are participating in DHS's US-VISIT Strategic Plan. DOJ and FBI are part of the team working on US-VISIT's Strategic Plan. The Strategic Plan will outline the business functionality needed for the immigration and border management enterprise, the technology, data, and facilities needed to support that functionality, and the business case that justifies the program. Providing DHS and DOS access to IAFIS information will be included as part of this US-VISIT Strategic Plan.

The following are recommendations that DHS would like to see added to the report:

1. IAFIS modernization should support DHS's operational needs. DHS would like an expanded role for DHS/Border and Transportation Security, US-VISIT, and DOS in the FBI's ongoing IAFIS modernization effort. As large customers of IAFIS, DHS would welcome the opportunity to inform the FBI of future requirements and operational needs. In particular, DHS would strongly emphasize the need to:

   - Improve availability/reliability (up time and failover);
   - Increase availability of terrorist prints;
   - Re-architect IAFIS and NCIC to allow searches by offense; and
   - Improve system capacity and system response time.

2. DHS would like the third recommendation in the draft report instead to ask the FBI to work with DHS to determine which IAFIS records are relevant in the determination of admissibility.

   DHS believes the FBI should immediately provide the relevant criminal history records to DHS. DHS is currently conducting a study to determine which records in IAFIS provide the highest value to immigration and border management decision makers so that access to these can be prioritized, while the more difficult interoperability challenges are architected. We were disappointed last year when the criminal history records of aliens of unknown origin were requested so that they could be included in our IDENT lookout database, and the answer was that it would take 720 days (the working draft says six years). It should be a top

priority to provide this information to DHS since this information has the highest relevancy for DHS's mission.

3. DHS and the FBI should finalize the Memorandum of Understanding (MOU) to clearly articulate how data should be shared and used, and to protect the privacy of our visitors. DHS has provided the FBI with access to US-VISIT and immigration violator data. DHS has provided user accounts to FBI analysts and provided extracts of data to IAFIS in support of DOJ operational needs. DHS did this in good faith that a memorandum of understanding will be agreed upon that provides for information sharing with DOJ/FBI and ensures that the necessary protections are clearly delineated so that DHS can ensure that the privacy of legitimate travelers is properly protected through explicit procedures for access to the data and normal audit provisions are included.

4. The FBI should actively work to improve the quality of IAFIS and NCIC data.

   - Provide final dispositions (i.e., not just fact of arrest);
   - Provide full criminal history response (FBI queries certain individual state repositories to get full recent criminal history information; FBI does not do so on all requests); and
   - Improve the quality of prints from local law enforcement officers (LEOs). Quality of the prints is the most important determinant of accuracy of matching. DOJ should ensure that state/local law enforcement is equipped to electronically capture and submit, in real time, high quality prints from those they arrest and prosecute.

APPENDIX VI
OIG ANALYSIS OF DHS COMMENTS

On November 19, 2004, the Office of the Inspector General (OIG) sent copies of the draft report to the Department of Homeland Security (DHS). The Undersecretary of Border and Transportation Security provided the DHS response in a letter and attached comments dated December 3, 2004 (Appendix V). None of the six recommendations in the report are directed to the DHS. However, because the report addresses DHS policies and operations, we offered the DHS an opportunity to comment on the report. Our analysis of the DHS comments follows.

Summary of DHS Comments Regarding Patriot Act Requirements: The DHS stated that the HSC Deputies Committee's July 18, 2003, decision to "establish as the technical standard for the US-VISIT Program" two fingerprints and a photograph constituted fulfillment of the Patriot Act requirements. The DHS also stated that the Patriot Act did not assign the NIST the sole responsibility for setting the technology standard. Regarding the Deputies' decision that the DOS, the DHS, and the OMB conduct planning for migration to an eight fingerprint system, the DHS stated that this was based on concern expressed by the NIST that when the US-VISIT database grows to a certain size, the result might be a large number of false positive fingerprint matches.[3] The DHS stated that the Deputies' decision did not relate to ten fingerprints and the use of IAFIS, and "the problem of false positives has not materialized." Lastly, the DHS stated that it is conducting appropriate planning to support the move to an eight-fingerprint system "when appropriate."

OIG Analysis: The July 18, 2003, HSC Deputies' decision, which appears in a document entitled "Summary of Conclusions," consists of the following statement: "With respect to the biometric identifier standards for the US-VISIT program, the Deputies approved the use of a photograph and two fingerprints for initial deployment in sea and airports. Deputies directed the Departments of Homeland Security and State to work with HSC and OMB in developing future plans to migrate to an eight fingerprint system." In light of DHS's comment, we added language describing the Deputies' decision to the Executive Summary of the report (we already had referred to the HSC Deputies' decision in the body of the report).

The DHS response demonstrates that the departments do not interpret the Deputies' decision or the requirements of the Patriot Act in the same way.

[3] The false positive rate, or false accept rate, is the probability that the system will incorrectly determine that a search fingerprint and a file fingerprint are matches.

The DOJ does not concur with the DHS contention that the Deputies' decision to authorize a two-fingerprint technology for initial US-VISIT deployment represents a decision on the final fingerprint collection standard for the US-VISIT program, or that the decision replaced the congressional mandate for the Secretaries of the DHS and DOS, working jointly with the NIST, to develop and certify a technology standard. The DOJ's position that the Deputies' decision was not meant to be the final fingerprint collection standard is based on the Deputies' direction that plans be made to migrate to an eight-fingerprint system. As described to us by DOJ officials, the HSC's decision was intended to allow the DHS to deploy US-VISIT quickly by taking advantage of the existing two-fingerprint IDENT system. While it is correct that the Deputies do not specifically mention a ten-fingerprint system, the congressional report that the NIST, Attorney General, and Secretary of State submitted to Congress in January 2003 stated that a standard based on ten flat fingerprints offered the most technologically and operationally acceptable approach for the Departments of Justice, Homeland Security, and State to screen incoming visitors. The varying interpretations reinforce our finding that the departments have failed to agree on a uniform fingerprint collection standard.

It is also important to note that the decision on a uniform fingerprint collection standard is required before further progress can be made on the efforts to achieve full interoperability of IDENT and IAFIS, efforts that are currently stalled. Because the decision has not been made, we recommended that the DOJ report to the HSC and Congress that the departments have reached an impasse and cannot complete the congressionally directed MOU to guide the integration of IDENT and IAFIS. We believe that the DOJ's report should formally request that the HSC or Congress decide whether or not to adopt the NIST Technology Standard (ten flat fingerprints for enrollment and two flat fingerprints and a photograph for identity verification). It is clear that a final decision on the adoption of a uniform fingerprint collection standard must occur before plans to make IAFIS and IDENT fully interoperable can be completed.

We agree, as the DHS commented, that the NIST was not assigned the sole responsibility for establishing the fingerprint technology standard, and we did not state otherwise in the report. In order to make clear that the NIST does not have sole responsibility for developing the technology standard, we amended the language on pages vi, 8, and 31 to reflect that Congress directed the Attorney General and Secretary of State, jointly through the NIST, to develop the technology standard.

Regarding the increasing number of false positives, the DHS correctly stated that NIST research determined that the number of false positive fingerprint matches would increase as the US-VISIT database grows. As we

stated on pages 31 and 32 of the report, the NIST also found that search accuracy increased (i.e., there were fewer false positives) when the maximum number of fingers (ten) was used to search a database. The NIST found that this was true for all fingerprint matching systems that it tested. We also noted in the report the DOJ's position that the most effective approach to addressing the issue of false positives is to increase the number of fingerprints collected for each person in the database before the number of false positives becomes a problem.

Summary of DHS Comments Regarding Success of US-VISIT: The DHS stated that both it and the DOS have engineered "the single most significant change to the visa issuance and U.S. border inspections process ever." Citing the over 13 million travelers that have been processed through US-VISIT, the DHS stated that at ports of entry, it has identified over 1,500 individuals who were on the US-VISIT watch list and denied entry to hundreds of them, and at consular posts, over 3,500 individuals have been identified through the US-VISIT watch list. The DHS stated that all of this has been accomplished while protecting traveler privacy and without increasing wait times or impacting trade and travel.

OIG Analysis: We acknowledge the DHS's statement that the first phase of US-VISIT is a significant achievement. The DHS reported that it identified 5,000 of 13,000,000 visitors as being on the US-VISIT watch list. However, as described in our report, the Metrics study conducted by the DOJ found that most aliens with criminal records could be identified only by checking the IAFIS Criminal Master File, not through IDENT alone, which is what US-VISIT checks. Of the 24,020 aliens identified by the Metrics study as having criminal records, 17,553 (73.1 percent) were identified only through IAFIS. Therefore, we recommended that the DOJ request a random sample of records from US-VISIT and other relevant immigration biometric databases to determine the additional number of criminals that IAFIS could identify if enrollments in US-VISIT were checked against IAFIS.

Summary of DHS Comments Regarding NIST Research on Time Requirements for Taking Ten Flat Fingerprints: The DHS stated that the draft report was misleading because it stated that the NIST research showed that ten "flat" fingerprints can be taken almost as quickly as two flat fingerprints. The DHS stated that readers would believe that the additional 10-15 seconds required to take ten fingerprints of 43 million visitors per year is operationally feasible. The DHS stated that even discounting the required processing time, the additional 10-15 seconds required to capture ten fingerprints would have "an enormous impact" and would require a significant number of additional inspectors, consular officers, and significant facility modifications to handle the

increased wait times. The DHS contended that the report therefore showed a lack of understanding of DHS and DOS operations.

OIG Analysis: Our report stated that the NIST's research found that 10 flat fingerprints can be taken in approximately 30 seconds (10 to 15 seconds longer than taking 2 flat fingerprints). As the OIG responsible for oversight of the Immigration and Naturalization Service (INS) before its transfer into DHS, and in light of the many reviews we conducted of the immigration process, we have a long and deep understanding of immigration operations. We understand that additional time to take ten flat fingerprints will have an effect on DHS and DOS operations. In our review, we also recognized that the significant time constraints that exist at primary inspection do not exist in secondary inspection or at the consulates where visa applications are taken, which the DHS response does not address. Importantly, although the DHS asserted that it is not operationally feasible to implement a ten-flat fingerprint system, it did not provide detailed information describing how many additional resources and facility modifications that it believes would be necessary if such a system was implemented, either in primary or secondary inspection.

However, as we noted in the report, the NIST studies we cite have indicated that taking ten fingerprints is the best technological solution to ascertaining the identify of individuals entering the United States. The critical issue to be determined is whether the operational costs would be justified by the benefits of implementing a ten-flat fingerprint system. Until the DHS grants the DOJ access to a random sample of data from US-VISIT and other relevant immigration biometric databases, the DOJ cannot conduct a proposed study (as we recommended to the DOJ) to determine the risk of not checking all visitors against IAFIS. Therefore, whether the cost of implementing a ten fingerprint system are justified because of the benefits that such a system will likely identify more criminal aliens by checking IAFIS directly cannot be compared at this point. We believe that the HSC and the Congress need that analysis to decide whether the risks constitute significant national security threats that warrant providing the DHS with the necessary resources and personnel to implement a ten-flat fingerprint system.

Lastly, the DHS stated that it is already conducting planning to support moving to an eight-fingerprint system, at the direction of the HSC. Therefore, the DHS objections regarding the additional processing costs are inconsistent because the DHS appears to believe that it will have to eventually address the issues of additional processing time and personnel costs, as well as potential facility modifications as a result of its own plans.

Summary of DHS Comments Regarding US-VISIT Architecture: The DHS stated that our report is misleading because it incorrectly equates the MitreTek

study of the FBI's IAFIS system with the DHS's IDENT system, but US-VISIT does not use the same architecture as IAFIS. The MitreTek study, the DHS stated, analyzed IAFIS's architecture, which requires using all ten fingerprints in order to filter the database down to a small enough size to compare the two index fingerprints. The DHS stated that IDENT does not use this type of filtering in its architecture, and that adding ten fingerprints to IDENT would add additional time to the process because IDENT would need to make more matches, not fewer.

OIG Analysis: We recognize that IDENT uses a different type of filtering in its architecture than IAFIS. Although in the report we presented a brief description of how fingerprint filtering in IAFIS works, we made no assumptions about the IDENT architecture. Our report cites a MitreTek study that found that searching a biometric database using two flat fingerprints results in longer processing times and reduced accuracy (a greater likelihood of identifying false positives) compared to using more fingerprints to conduct the searches, and NIST findings that providing more fingerprints substantially speeds search processing and increases search accuracy. The need to ensure that compatible architectures can be integrated is a primary reason for timely resolving the issues we raise in this report.

In addition, because the DHS did not earlier communicate to us its contention that adding ten flat fingerprints to IDENT would increase rather than reduce processing time, we contacted the manager of the NIST Image Group to discuss this issue. In response to our inquiry, he contacted a contractor involved in developing IDENT, and then responded to us that implementing a ten-flat fingerprint system would cause about a 20 percent increase in the time taken by the IDENT fingerprint matching process. However, he stated, the operational impact of such an increase in the matching process would likely be negligible because the computer processing time is only a part of the fingerprint check. In sum, the biometrics experts at the NIST and the DHS will need to address this issue fully in order to determine the extent to which an increase in the fingerprint matching process could affect the DHS's operations.

Summary of DHS Comments Regarding IDENT/IAFIS: The DHS stated that our report incorrectly assumes that the US-VISIT program has the same set of requirements that generated the need for IDENT/IAFIS. The DHS stated that the component of IDENT that US-VISIT uses is a "traveler identification system with lookout capability," which is not designed for booking criminals. The primary US-VISIT database, the DHS stated, contains the biometrics of over 10 million enrolled legitimate foreign travelers, which is separate from the IDENT lookout database that receives daily extracts from IAFIS. The DHS stated that IDENT/IAFIS was originally intended to provide quick access to

criminal history information to INS officers during apprehension, but that future versions were to give state and local law enforcement organizations access to IDENT immigration information. Lastly, the DHS stated that the US-VISIT database does not contain immigration violators.

OIG Analysis: We did not assume that the US-VISIT program has the same set of requirements that generated the need for IDENT/IAFIS. Our report makes clear that the US-VISIT and IDENT databases are separate and that it is the US-VISIT watch list that is being queried when visitors apply for a visa or arrive to be inspected. The report explains that the US-VISIT watch list includes the IDENT lookout database, which, as the DHS stated, contains data extracted from IAFIS. However, the information extracted into IDENT is only a small portion of all the records in IAFIS. The majority of the estimated 43 million annual visitors to the United States are not checked directly against IAFIS – which contains the most current and complete criminal history information – but are only checked against the US-VISIT watch list. The risk of this practice is that some known criminals will be missed, as the DOJ's Metrics study showed, because the extracts included in IDENT are not complete and are prone to have errors and omissions.

Therefore, while it is correct that the US-VISIT is not intended to be a booking system for criminals, it should still be as effective as it can be at identifying whether visitors have criminal records or are suspected terrorists. However, neither the potential for a ten-fingerprint system to identify more criminal aliens among visitors to the United States, nor the potential additional costs of implementing a ten-fingerprint system are known at this point. As we stated above, we believe that the HSC and the Congress need that information in order to decide whether the operational and financial costs of implementing a ten-flat fingerprint system outweigh the benefits of implementing such a system.

Summary of DHS Comments Regarding IAFIS's Ability to Meet DHS Operational Requirements: The DHS stated that our report incorrectly assumes that the FBI's IAFIS system could be used for US-VISIT purposes and that taking ten fingerprints for every traveler at ports of entry and submitting these to the FBI's IAFIS "would solve most of the interoperability issues and would be beneficial." The DHS stated that this assumption is inaccurate because it believes IAFIS, as currently established, cannot meet DHS operational requirements for several reasons, which the DHS listed:

- Not all criminal history records are relevant to all DHS decisions. The DHS included an example stating that its analysis has shown that only a small percentage of the wanted person's information in IAFIS has a bearing on whether the individual will be admissible to the U.S., and

immigration officers in primary inspection do not have the time or need to review the vast majority of these records.

- IAFIS' response time on a Ten Print Rap Sheet Request (TPRS) query is approximately 10 minutes versus 10 seconds for US-VISIT at primary inspection.

- IAFIS does not have the capacity to handle the volumes associated with US-VISIT. The DHS stated that there could be up to 180,000 transactions per day, which would be nearly 10 to 20 times the current capacity of a TPRS search through IAFIS.

- IAFIS' availability is not adequate for real-time operations. The DHS cited two days per month of IAFIS downtime (planned and unplanned) over the last six months and stated that planned outages have recently been occurring almost monthly. The DHS also stated that unscheduled outages are a significant problem for IAFIS; it provided an example of IAFIS being down numerous times, including one time for two hours, in the two weeks prior to their response.

- IAFIS does not have any backup capability as our report noted. The DHS stated that IAFIS resides in a single location, with tapes stored off-site. It would be impossible, the DHS stated, to bring the system back on line in a reasonable amount of time, should something happen to its primary location. The DHS stated that US-VISIT IDENT has "redundant search capability" in Rockville, Maryland and Dallas, Texas, with "failover capability" between the two locations.

- The costs of moving to an FBI-based ten-fingerprint solution are significant and with little benefit to the DHS, given the FBI's current inability to respond to the DHS's operational time constraints with focused and relevant information. The DHS stated that even discounting the significant cost to the FBI that would be required to expand IAFIS capacity, the costs to the DHS are prohibitive; the DHS stated that capturing ten fingerprints would require hundreds of additional inspectors and significant facility modifications at the ports.

Finally, the DHS stated that it does not believe that there would be cost savings for moving immediately to a ten-fingerprint system because the costs would be far greater than DHS's initial investment of $70 million for US-VISIT IDENT, and $15 million annual operating costs. The DHS stated that it recognizes that biometric technology is constantly evolving, and although it is not technically or economically feasible to implement a change now, with advances in fingerprint capture and matching technology it may be technically feasible to move to a multi-print system in the future. However, the DHS

stated that even if it were possible, the "potential huge disruption to the travel and tourism industry, due to increased processing times and cultural resistance associated with criminality," must be analyzed before the DHS would make the significant investments to move to a ten-print system.

OIG Analysis: Regarding the DHS's first point that not all criminal history records are relevant to all DHS decisions, having access to all criminal records would enable immigration officers to make the most informed decision possible. Currently, consular and immigration officers do not have full access to the most current and complete records contained in IAFIS. Should such access be granted, the immigration officer first would be alerted to a possible fingerprint match and then the visitor would be referred to secondary inspection where the information would be evaluated.

The DHS's reference to response time is a legitimate concern for primary inspections, and our report makes this point. The FBI stated that IAFIS would provide a TPRS response time of less than 10 minutes and currently the system is averaging 2-3 minutes, although 2 minutes is currently the fastest response time it can produce. However, adjudications that occur in secondary inspections or in consular offices do not have the same time constraints as primary inspection points. Secondary inspections involve checking other databases and questioning the visitor. Therefore, as is the case with processing time, the TPRS transaction response time is much less of an issue for officers working at secondary inspection and the consular offices.

Regarding IAFIS capacity, we agree with the DHS that IAFIS does not presently have the capacity to handle the volume of transactions associated with US-VISIT. Part I of the report makes this point clearly. Nonetheless, we believe that is it important to fully utilize existing IAFIS capacity. Moreover, decisions on future requirements are needed to enable the FBI to ensure that IAFIS will be prepared to handle a large increase in transactions associated with US-VISIT. We recommended that the DOJ and the FBI coordinate with the DHS to identify the capacity needed to conduct IAFIS searches on all visitors referred to secondary inspection. The DOJ and the FBI concurred with this recommendation.

Regarding IAFIS availability, we agree with the DHS that IAFIS must improve its availability. Part I of the report makes this point clearly. We also made a recommendation that the FBI take steps to ensure that IAFIS meets its system availability requirements of 99 percent; both the DOJ and the FBI concurred with this recommendation.

Regarding the lack of IAFIS backup, we discuss this at some length in Part I of the report. In addition, on page 28 of the report, we added a footnote

containing the information that the DHS provided about the redundant US-VISIT and IDENT search capability.

Regarding the DHS conclusion that the costs of implementing a ten-fingerprint system are significant and provide little benefit, we believe that conclusion is both premature and not clear. Our report recognized that there would be additional costs to the DHS and the DOS in order to implement a system that takes more than two fingerprints. However, neither the potential for a ten-fingerprint system to identify more criminal aliens among visitors to the United States, nor the potential additional costs of implementing a ten-fingerprint system are known at this point.

Regarding the DHS statement that it is erroneous that there would be any cost savings associated with expediting the implementation of a ten-fingerprint system, a number of potential savings that could result from such a decision were identified to us during this review. These include eliminating or reducing the cost of maintaining duplicate data in redundant systems; reduced costs of processing ten fingerprints against ten fingerprints, rather than processing two against ten (as cited by the NIST and others); and operational savings (and reduced inconvenience to visitors) from reducing the number of false positive matches. There are also potential costs associated with delaying implementation of a ten-fingerprint system. Those include operational and financial costs to re-engineer the fielded systems and re-enroll individuals using more than two fingerprints.

The DHS stated that delays would likely occur at primary inspection due to slow IAFIS response times, which it believed would be disruptive to the travel and tourism industry. However, some disruption will likely result in conjunction with any procedural change that the DHS implements, whether now or in the future. Moreover, should an incident occur involving a criminal alien or terrorist inadvertently admitted to the United States, which is a viable risk, the DHS and the DOS would likely experience greater pressure to move more quickly to a re-engineered system, and would be at risk of implementing rushed or inadequate measures. We believe that by effectively planning for implementation of a system that uses more than two fingerprints – including completing the MOU with the DOJ – the DHS and the DOS can better ensure that costs and disruptions are minimized. Moreover, as stated above, the HSC and the Congress need an analysis of both the potential costs and the risks of not checking all visitors against IAFIS to decide whether they warrant expending additional resources for the DHS to implement a ten-flat fingerprint system and to accommodate the additional processing time. Only after the results of this study are analyzed will the federal government be able to fully assess the costs and benefits of a ten-fingerprint system.

Summary of DHS Comments Regarding JMD Criminality Study: The DHS stated that the findings of the JMD criminality study cannot be extrapolated to the US-VISIT population. The DHS stated that our report incorrectly compares the results from JMD's Metrics study and US-VISIT because the two populations are fundamentally different; US-VISIT contains information on travelers while the individuals in the JMD study had already been arrested by the Border Patrol. The DHS stated that these individuals have already shown a disregard for the law by crossing the Border illegally. The DHS added that it already had accelerated the deployment of the fully integrated IDENT/IAFIS terminal to all Border Patrol locations.

OIG Analysis: We agree that the visitors in US-VISIT and the sample of aliens examined by the Metrics study are different. The Metrics study found that about one in eight of the aliens detained by the Border Patrol and checked in the Metrics study had a criminal record. According to data cited by the DHS in its response, the US-VISIT has identified about 5,000 of the 13,000,000 visitors checked so far (about 1 in every 2,600 visitors) as being on the US-VISIT watch list. Although the US-VISIT watch list is not a comprehensive list of criminals and other individuals ineligible to enter the United States, these results indicate that the percentage of the general population of US-VISIT visitors who have criminal records (the criminality rate) is less than that of the aliens examined in the Metrics study. We are aware of these differences and, for that reason, we did not extrapolate the criminality rate found in the JMD Metrics study to the US-VISIT population.

Nonetheless, the findings of the Metrics study regarding the capability of IDENT and IAFIS to identify criminal aliens are relevant. The Metrics study clearly showed that only checking IDENT (which the US-VISIT watch list relies on) will fail to identify most criminal aliens. Over 70 percent of the criminals identified in the Metrics study were only identified by IAFIS. While we agree that the criminality rate of US-VISIT visitors may be lower than the Metrics study, neither the actual US-VISIT criminality rate nor the percentage of criminals that are missed by US-VISIT is known. It is for that reason that we recommended that the DOJ conduct a study using random samples from US-VISIT and from other relevant immigration biometric databases used for enforcement or benefit purposes to determine the additional number of individuals that IAFIS will identify as criminals and the risk posed by not checking all visitors against IAFIS.

Summary of DHS Comments Regarding Organizational Responsibility: The DHS stated that the draft report cited the DOJ and the DOS as being responsible for implementing appropriate biometric standards under the Border Security Act, but that this responsibility has now been transferred from the DOJ to the DHS. The DHS also stated that it has developed an "alternative

proposal" for addressing the need for IDENT/IAFIS interoperability, especially in relation to US-VISIT, which is designed to achieve appropriate data exchange between the DOJ and the DHS.

OIG Analysis: The DHS is correct about the shifting of organizational responsibility from the DOJ to the DHS. On pages iv and 8 of the report, we added a footnote to the description of the Border Security Act that clarifies this shift in responsibility. Regarding the "alternative proposal," the DHS has provided us with no information on this.

Summary of DHS Comments Regarding Monitoring IDENT Performance: The DHS stated that it and the DOS are aware of both the capabilities and limitations of the biometric systems employed by US-VISIT. The DHS stated that it continues to closely monitor the IDENT system and work with the NIST with the goal of improving system performance, including false positive rates, accuracy rates, and system throughput. The DHS stated, "We will move to a multi-print system at the appropriate time to improve system performance."

OIG Analysis: We accept the DHS statement that it closely monitors US-VISIT and works with the NIST. However, because we found that the DHS, the DOS, and the DOJ did not interpret the HSC Deputies' decision or the Patriot Act requirements in the same way, and because the departments continue to disagree on a uniform fingerprint collection standard, no further progress toward achieving full interoperability between IDENT and IAFIS can be made.

It has been almost two years since the NIST, the Attorney General, and the Secretary of State issued the report to Congress stating that ten flat fingerprints is the most effective and efficient method of enrolling individuals in large biometric databases. Similarly, it has been almost one and a half years since the HSC Deputies' approved the use of two flat fingerprints and a photograph for initial US-VISIT deployment, with the direction to conduct planning for the eventual migration to an eight-fingerprint system. The DHS stated it is already conducting this planning. However, the departments have as yet been unable to complete an MOU to establish how the project to achieve interoperability will proceed. The recommendations we make are partly intended to improve the information available to the HSC and Congress regarding the risks and costs associated with the various options so that they may better examine the issues related to the fingerprint technology standard and capabilities required for an interoperable biometric fingerprint system.

Summary of DHS Comments Regarding US-VISIT Strategic Plan: The DHS stated that the DOJ and the FBI are part of the team working on US-VISIT's Strategic Plan, which will "outline the business functionality needed for the immigration and border management enterprise, the technology, data, and

facilities needed to support that functionality, and the business case that justifies the program." The DHS stated that providing the DHS and the DOS with access to IAFIS information is part of the US-VISIT Strategic Plan.

OIG Analysis: The US-VISIT Strategic Plan team is a recently formed group that we did not review during our fieldwork. However, based on discussions with DOJ staff, we added this group to the report's list of working groups on page 18.

Summary of DHS Comments Regarding Recommendations to be Added to the Report: The DHS stated that it would like the following recommendations added to the report.

1. "IAFIS modernization should support DHS's operational needs." The DHS stated that it would like an expanded role for DHS/Border and Transportation Security, US-VISIT, and the DOS in FBI's ongoing IAFIS modernization efforts. As large customers of IAFIS, the DHS stated that it would welcome the opportunity to inform the FBI of future requirements and operational needs, including the need to:

    - Improve availability/reliability (up time and failover).
    - Increase availability of terrorist prints.
    - Re-architect IAFIS and NCIC to allow searches by offense.
    - Improve system capacity and system response time.

OIG Analysis: Improving IAFIS availability and increasing the availability of terrorist fingerprints are already recommendations in our report. Although re-engineering IAFIS and NCIC to allow searches by offense may be beneficial, this is the first time that the DHS has raised this issue to us, and it is outside the scope of this report. Improving IAFIS capacity is also addressed in the report and is already addressed in our recommendations. Reducing IAFIS response time is a goal of Next Generation IAFIS, but DOJ, FBI, and DHS technical experts will have to determine how IAFIS can meet the response time required at primary inspection.

2. "DHS would like the third recommendation in the report instead to ask the FBI to work with DHS to determine which IAFIS records are relevant in the determination of admissibility." The DHS stated that it believes that the FBI should immediately provide the relevant criminal history records to the DHS. The DHS stated that it is currently conducting a study to determine which IAFIS records provide the highest value to immigration officials so that they may prioritize their access while the more difficult interoperability challenges are architected. The DHS stated that it was disappointed when it requested the criminal history

records of aliens of unknown origin from the FBI and was told that it would take 720 days. The DHS believes that it should be a top priority for the FBI to provide this information to the DHS.

OIG Analysis: This DHS comment is unrelated to the random sampling of US-VISIT that our report recommends. We do describe the fingerprint image requests and the DHS's desire to prioritize them. We also understood that the US-VISIT watch list may not have the capacity to handle the estimated 7 million additional records of individuals who are foreign born, have no place of birth listed, or who have had previous encounters with immigration officials documented in IAFIS. Moreover, the DHS's expectation that the FBI should provide all of these records to the DHS is indicative of its position that the current interim measure involving the FBI extracting data from IAFIS and providing it to the DHS for inclusion in IDENT is adequate. As our report states, the DOJ does not believe that providing extracts of IAFIS data achieves interoperability; rather, the extract process is an inadequate method of checking individual's criminal history because the extracts are untimely, erroneous, and incomplete. The extract process also creates data duplication.

The FBI sent a letter to the US-VISIT Program Manager in February 2004 stating that a mass extract of the types of records (described above) that the DHS requested would require 750 days to process with current IAFIS capacity. However, the FBI told us that it would take many years to extract the entire population in which the DHS has an interest. We state in the report that since the DHS is permitted to extract 3,000 records a day from IAFIS, by dividing 3,000 into 7 million we estimate that it will take over 6 years to accomplish.

3. "DHS and the FBI should finalize the Memorandum of Understanding (MOU) to clearly articulate how data should be shared and used, and to protect the privacy of our visitors." The DHS stated that it has provided: (1) the FBI with access to US-VISIT and immigration violator data, (2) user accounts to FBI analysts, and (3) extracts of data to IAFIS in support of DOJ operational needs. The DHS stated that it did this in good faith that an MOU would be agreed upon that provides for information sharing with the DOJ/FBI and ensures that the necessary privacy protections and data access procedures are clearly delineated.

OIG Analysis: We agree that the DHS and the FBI should finalize such an MOU. On page 37 of the report, we added language discussing the DHS's November 1, 2004, memorandum to the HSC Deputy Director, which stated that it had met its obligations to provide the FBI with full access to its US-VISIT records. In the memorandum, the DHS stated that it had provided training on the data limitations of US-VISIT records to 30 individuals named by the FBI. In the memorandum, the DHS also stated that it would provide US-

VISIT access and training to an additional 200 users whom the FBI indicated also need access to US-VISIT.

However, DOJ officials told us that they are disappointed at the slow pace and limited scope of the access that the DHS has provided thus far and do not consider that the FBI has "full and immediate" access to the US-VISIT database. Further, DOJ officials stated that they considered the DHS's granting access to 30 FBI individuals a short-term, stop-gap measure intended to provide limited access to certain FBI users quickly. Our report also states that little progress has been made toward providing the DHS's apprehension and criminal history information to other federal, state, and local law enforcement agencies. Based on our discussions with officials in all the departments, as described in this report, we concluded that the efforts to ensure that the information in the DHS's IDENT and US-VISIT databases will be "readily and easily accessible," (as required by the Patriot Act), to the DOJ or other federal, state, and local law enforcement agencies have stalled.

4. "The FBI should actively work to improve the quality of IAFIS and NCIC data" so that it would:

- Provide final dispositions,
- Provide full criminal history response, and
- Improve the quality of fingerprints from local law enforcement officers because fingerprint quality is the most important determinant of matching accuracy. The DHS stated that the DOJ should ensure that state and local law enforcement is equipped to electronically capture and submit, in real time, high quality fingerprints from individuals they arrest and prosecute.

OIG Analysis: The first time that the DHS has raised these issues to us was in their response to our draft report. We contacted responsible FBI officials, and they told us that the FBI is working on these issues to the extent that they are within its area of responsibility and authority. However, these issues are not within the scope of this report.

APPENDIX VII
DOS COMMENTS ON THE DRAFT REPORT

United States Department of State

Deputy Assistant Secretary
for Visa Services

Washington, D.C. 20522-0113

December 3, 2004

Mr. Glenn A. Fine
Inspector General
Office of the Inspector General
Department of Justice
Washington, DC 20530

Dear Mr. Fine:

We appreciate the opportunity to comment on this latest draft of the report entitled, *IDENT/IAFIS: Follow-up Review of the Status of IDENT/IAFIS Integration.* On November 16 I sent you a letter with comments concerning an earlier draft of the report. This letter will provide some additional comments while reiterating some of the views in my earlier letter. Please append my two letters to your report so that readers will be aware of the scope of views on the important subjects the report addresses.

The draft continues to present fundamental inaccuracies on the technology standard, as evidenced by the statement on page 17: "The Commerce Department's NIST has statutory authority to develop and certify a Technology Standard that includes biometrics, in order to verify the identity of individuals applying for a visa or using a visa to enter the United States." This sentence should be struck. As mentioned in my November 16 letter, by section 403(c) of the USA PATRIOT Act, the Secretary of State and the Attorney General--not the NIST--are granted the statutory authority to set the technology standard. While the policy makers must take into consideration recommendations of the NIST, the NIST is assigned only a technical advisory role in the decision-making process. On July 18, 2003, the HSC Deputies Committee decision to adopt the two-print standard reflected the exercise of that statutory authority. Although the current version of the report does contain a footnote of the HSC's decision, such a significant fact should be moved to the body of the text. It is the HSC decision, not the NIST advice, that controls DOS, DHS and DOJ implementation of a technology standard.

Throughout the report there are a number of references to the failure of DOS and DHS to implement the technology standard of NIST. All such references should be struck. DOS and DHS are implementing the July 18,

2003, HSC Deputies Committee decision on the technology standard, which remains in effect.

The draft report ignores other important facts. For example, when NIST asserts that taking 10 flat prints takes only 10 to 15 seconds longer than taking two flat prints, that increased time may not appear to be a relevant factor in the NIST laboratory environment, but its effect on operations at a port of entry would be significant. Moreover, the Department of State is presently conducting a pilot involving collection of 10 flat prints at our Consulate General in Monterrey, Mexico, from visa applicants whose names match NCIC entries in the Consular Lookout and Support System (CLASS). With a Consulate General employee assisting the person whose fingerprints are being enrolled, it is taking 60 to 90 seconds to enroll 10 flat prints. That is 30 to 60 seconds longer than it takes to enroll two flat prints without any assistance. Adding one minute of processing time to 7,000,000 visa applications annually has significant workload implications.

Furthermore, because enrollment of 10 flat prints would require shifting the enrollment process off-site at some consular posts, facilities and personnel costs would skyrocket. It is not the responsibility of NIST to consider these operational and cost factors; that is why the statutory authority for such decisions rests with agency heads, with NIST providing technical information for consideration.

Another pilot that the Department of State is undertaking with the cooperation of the FBI provides an automated process for obtaining rap sheets for visa applicants whose fingerprints are on the IDENT watchlist. Under this pilot, which is currently deployed to our embassy in San Salvador, El Salvador, when the two fingerprints collected from the visa applicant under the Biometric Visa Program match two fingerprints on the IDENT watchlist that refer to an FBI file number, the two fingerprints are then routed back through the Consular Consolidated Database (CCD) to IAFIS for a match against the prints in the FBI file, which results in the rap sheet being sent automatically to the CCD to be transferred to the post.

In my November 16 letter to you I outlined a three-step process for transferring fingerprints from IAFIS to IDENT. The two-print pilot being tested at Embassy San Salvador could be deployed globally in conjunction with that three-step process to enable fully automated access by consular officers to rap sheets on visa applicants through biometric identity

verification. This would be a main component of the "interoperable electronic data system to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also know as the 'Chimera system')" envisioned in section 202 of the Enhanced Border Security and Visa Entry Reform Act.

To recount from my November 16 letter, the three-step process to achieve the realization of this system consists of:

1) Implementation of the initiative by the Department of Homeland Security to develop a means to prioritize the 7-8 million records of foreign-born persons contained in IAFIS. This initiative would allow for the fingerprints of persons with the most serious criminal history records, e.g., homicide, to be transferred first to IDENT.

2) Expansion of the Image Request Services function of IAFIS, which now has a daily capacity to transfer out 7,000 fingerprints, of which 3,000 are allotted to IDENT, to a much greater transfer capacity.

3) Upgrade of the connectivity between IAFIS and IDENT to be able to handle a rapid daily transfer of many thousands of fingerprint files.

To prepare for undertaking steps 2 and 3, we recommend that a consultant be hired to conduct a study of the technical issues involved, with proposals for solutions and cost estimates.

We believe this three-step proposal would cost a fraction of the DOJ proposals to collect 10 fingerprints of visa applicants to be cleared against IAFIS. Most important, our proposal would keep intact the highly successful Biometric Visa and US-VISIT Programs, which the DOJ 10-fingerprint proposals would unnecessarily dismantle in their present forms. The importance of maintaining the Biometric Visa Program in its present form is that it allows the consular officer to focus attention on the visa interview. To require consular officers to detract time from visa interviews in order to expend countless hours of time collecting ten fingerprints would be detrimental overall to our border security.

The Departments of State, Homeland Security, and Justice share a common goal -- to screen visa applicants against criminal history records that would render them ineligible for visas. Of the options available to achieve that goal, we believe our proposal for enhancing the two-print system, which has already been decided upon by the HSC and has proved so successful for border security, would achieve that common goal most effectively and efficiently.

Sincerely,

Janice L. Jacobs

APPENDIX VIII
OIG ANALYSIS OF DOS COMMENTS

On November 19, 2004, the Office of the Inspector General (OIG) sent copies of the final draft report to the Department of State (DOS). The Deputy Assistant Secretary for Visa Services provided the DOS response in a letter dated December 3, 2004 (Appendix VII). None of the six recommendations in the report are directed to the DOS. However, because the report addresses DOS policies and operations we offered the DOS an opportunity to comment on the report. Our analysis of the DOS's comments follows.

Summary of DOS Comments Regarding Technology Standard: The DOS stated that our report presents "fundamental inaccuracies" on the technology standard because it states that the NIST has statutory authority to develop and certify a Technology Standard, which implies that the NIST solely has this authority. The DOS stated, "by section 403(c) of the USA PATRIOT Act, the Secretary of State and the Attorney General -- not the NIST -- are granted the statutory authority to set the technology standard." The DOS further stated "the NIST is assigned only a technical advisory role in the decision-making process."

OIG Analysis: As noted above, it is correct that the NIST was not assigned the sole responsibility for establishing the technology standard. On pages 8 and 31 of our report, we acknowledged the language of section 403(c) of the Patriot Act, which states that "the Attorney General and the Secretary of State jointly, through the [NIST]…" shall develop and certify a technology standard. After extensive testing to determine the most efficient and effective method for verifying the identify of visa applicants, the NIST recommended to Congress (in a January 2003 report issued jointly by the NIST, the Attorney General, and the Secretary of State) that ten flat fingerprints be used for enrollment into large databases and two flat fingerprints and a photograph only be used to verify individuals' identities against existing records. Thus, we refer to this as the NIST-recommended Technology Standard.

In order to make clear that the NIST did not have sole responsibility for developing the technology standard, we amended the language on pages vi, 8 and 31 to reflect that Congress directed the Attorney General and Secretary of State, jointly through the NIST, to develop the technology standard.

Summary of DOS Comments Regarding HSC Deputies' Decision: The DOS stated that the July 18, 2003, HSC Deputies Committee decision to use a two-fingerprint and photograph system for initial US-VISIT deployment in sea and air ports of entry reflected the Secretary of State's and the Attorney

General's statutory authority to set the technology standard. The DOS stated that "it is the [HSC] decision, not the NIST advice that controls DOS, DHS and DOJ implementation of a technology standard."

OIG Analysis: As we stated in response to the DHS's comments, the DOS response further demonstrates that the departments do not interpret the Deputies' decision or the requirements of the Patriot Act in the same way. The DOJ does not concur with the DHS and DOS contention that the Deputies' decision to authorize a two-fingerprint technology for initial US-VISIT deployment represents a decision on the final fingerprint collection standard for the US-VISIT program, or that the decision replaced the congressional mandate for the Secretaries of the DHS and State, working jointly with the NIST, to develop and certify a technology standard. The DOJ's position that the Deputies' decision was not meant to be the final fingerprint collection standard is based on the Deputies' direction that plans be made to migrate to an eight-fingerprint system. As described to us by DOJ officials, the HSC's decision was intended to allow the DHS to deploy US-VISIT quickly by taking advantage of the existing two-fingerprint IDENT system. The varying interpretations contained in the departments' responses reinforce our finding that the departments have not agreed on a uniform fingerprint collection standard.

The decision on a uniform fingerprint collection standard is required before further progress can be made on the development of an MOU to guide the efforts to achieve full interoperability of IDENT and IAFIS, efforts that are currently stalled. Because the decision has not been made, we recommended that the DOJ report to the HSC and Congress that the departments have reached an impasse and cannot complete the congressionally directed MOU to guide the integration of IDENT and IAFIS. We specified that the DOJ's report formally request that the HSC or Congress decide whether or not to adopt the NIST Technology Standard (ten flat fingerprints for enrollment and two flat fingerprints and a photograph for identity verification) because the adoption of a uniform fingerprint collection standard must occur before plans to make IAFIS and IDENT fully interoperable can be completed.

In previous comments provided to us on a working draft of this report, the DOS acknowledged that the NIST expressed concern that when the US-VISIT enrollment database grows to a certain size, a large number of "false positive" fingerprint matches would occur. In this response, the DOS stated that the problem of false positives has not materialized. The DOS is correct that NIST research determined that the number of false positive fingerprint matches would increase as the US-VISIT database grows. As we stated on pages 31 and 32 of the report, the NIST also found that search accuracy improved (there were fewer false positives) when the maximum number of

fingers (ten) was used to search a database. The NIST found that this was true for all fingerprint matching systems that it tested. We noted in the report the DOJ's position that the most effective approach to addressing the issue of false positives is to increase the number of fingerprints collected before the number of false positives becomes a problem.

Summary of DOS Comments Regarding Time Required to Take Ten Fingerprints: The DOS stated that by presenting the NIST finding that taking 10 flat fingerprints takes 10 to 15 seconds longer than taking two flat fingerprints, our report ignores the significant effect on operations at ports of entry that this additional time would have. The DOS also stated that at its consulate in Monterrey, Mexico, it is conducting a pilot project to collect ten flat fingerprints from certain visa applicants. The DOS stated that with a consulate employee assisting the person whose fingerprints are being enrolled, it takes 60 to 90 seconds to enroll 10 flat prints. That is, they say, 30 to 60 seconds longer than it takes to enroll two flat fingerprints without the assistance of a consular employee and has significant workload implications.

OIG Analysis: The independent NIST research found that taking 10 flat fingerprints only takes approximately 10 to 15 seconds longer than taking 2 flat fingerprints. We amended page 16 of the report to reflect that the DOS is currently conducting several pilot projects in Mexico to take ten flat fingerprints. However, we do not have enough information on the structure, process, or equipment used in the DOS pilot projects to evaluate whether they are similar to that used by the NIST in its studies. More importantly, the results of these pilot projects are not yet conclusive and the reasons for the enrollment time that the DOS has experienced thus far have not yet been identified or analyzed. We recognize that enrollment time is an important issue for the DOS. However, unlike the DHS inspectors at primary inspection, consular officers do not have to make an immediate adjudication.

Summary of DOS Comments Regarding Resources: The DOS stated that because enrollment of ten flat fingerprints would require shifting the enrollment process off-site at some consular posts, "facilities and personnel costs would skyrocket." These operational and cost factors, the DOS stated, are not the responsibility of the NIST; they are decisions to be made by agency heads.

OIG Analysis: Our report recognized that there would be additional costs to the DHS and the DOS in order to implement a system that takes more than two fingerprints. However, the DOS did not provide detailed information describing the facilities and personnel costs that it believes would be necessary if such a system is implemented. In fact, neither the potential for a ten-fingerprint system to identify more criminal aliens among visitors to the United

States, nor the potential additional costs of implementing a ten-fingerprint system are known at this point.

As we noted in the report, the NIST studies we cite have indicated that taking ten fingerprints is the best technological solution to ascertaining the identify of individuals entering the United States. The critical issue to be determined is whether the operational costs would be justified by the benefits of implementing a ten-flat fingerprint system. Until the DHS grants the DOJ access to a random sample of data from US-VISIT and other relevant immigration biometric databases, the DOJ cannot conduct a proposed study (as we recommended to the DOJ) to determine the risk of not checking all visitors against IAFIS. Therefore, whether the cost of implementing a ten fingerprint system is justified by the potential for such a system to identify more criminal aliens by checking IAFIS directly cannot be fully known at this point. We believe that the HSC and the Congress need that analysis to decide whether the risks constitute significant national security threats that warrant providing the DOS with the necessary resources and personnel to implement a ten-flat fingerprint system.

Moreover, on page 48 of our report we present the DOJ position that the federal government may face significant costs to later re-engineer existing systems if changes are not implemented now to upgrade US-VISIT to collect more than two fingerprints. These costs may include re-enrolling individuals when it is decided to begin using more than two fingerprints. A number of potential savings that could result from such a decision were also identified to us during this review. These include eliminating or reducing the cost of maintaining duplicate data in redundant systems; reduced costs of processing ten fingerprints against ten fingerprints, rather than processing two against ten (as cited by the NIST and others); and operational savings (and reduced inconvenience to visitors) from reducing the number of false positive matches.

Summary of DOS Comments Regarding Additional Pilot Study: The DOS described another pilot project at the embassy in San Salvador, El Salvador, that it is conducting in conjunction with the FBI. This pilot, the DOS stated, involves taking two fingerprints from certain visa applicants whose fingerprints are on the IDENT watch list, and automatically receiving the rap sheets for these applicants. The DOS described a three-step process for transferring fingerprints from IAFIS to IDENT and stated that the two-fingerprint pilot being tested in El Salvador could be deployed globally in conjunction with the three-step process to give consular officers fully automated access to visa applicants' rap sheets. This, the DOS stated, would be a main component of the interoperable electronic data system envisioned in the Border Security Act.

The three-step process that the DOS referred to consists of (1) a DHS initiative to prioritize the 7-8 million records of foreign-born individuals contained in IAFIS before transfer into IDENT, (2) an expansion of IAFIS's 3,000 daily image request services function, and (3) an upgrade of the IAFIS and IDENT connectivity "to be able to handle a rapid daily transfer of many thousands of fingerprint files." The DOS recommended that a consultant be hired to conduct a study of the technical issues involved with the second and third items, and to propose solutions and cost estimates. The DOS stated it believes that this three-step process would cost "a fraction of the DOJ proposals" and would "keep intact the highly successful Biometric Visa and US-VISIT Programs, which the DOJ [ten-] fingerprint proposals would unnecessarily dismantle in their present forms." The DOS stated that requiring consular officers to collect ten fingerprints would detract time from visa interviews and would be detrimental to border security. Lastly, the DOS restated its position that its proposal for enhancing the current two-fingerprint system would achieve the DOS, DHS, and DOJ common goal of screening visa applicants against criminal history records that would render them ineligible for visas.

OIG Analysis: The three steps that the DOS described all rely on the existing interim measures and do not present a long-term solution for fingerprint biometric interoperability, which according to the DOJ relies on multi-directional, direct, real-time access between the FBI, the DHS, and other law enforcement agencies needing access to immigration records. Checking a visa applicant's fingerprints against IDENT means that the individual's fingerprints are *not* checked directly against the FBI's IAFIS, which is the largest, most current, and most complete file of criminal fingerprints.

The DOS's response is consistent with its position that the current interim measure involving the FBI extracting data from IAFIS and providing it to the DHS for inclusion in IDENT is adequate. As we report, the DOJ does not agree that providing extracts of IAFIS data achieves interoperability; rather, the extract process is an inadequate method of checking individual's criminal history because the extracts are untimely, erroneous, and incomplete. The extract process results in the creation and maintenance of redundant databases.

The fact that the DHS is developing a prioritization method for the 7 million-plus records of foreign-born individuals suggests that it cannot currently support the entire file. As we stated on page 45 of our report, the current daily transfer will take 6 years to complete. According to the DOJ, this problem could be avoided by directly accessing IAFIS rather than waiting for the FBI to transfer, one day at a time, portions of the entire file. Further, upgrading IAFIS will not ameliorate the faulty extract process. Even with an

upgraded capacity, the FBI would still have to continue providing the DHS with regular extracts of its data, which the DOJ's Metrics study report found is incomplete and error prone.

Regarding the two DOJ proposals that the DOS cited, our report describes a draft proposal that the DOJ submitted to the Policy Coordination Committee containing two options and cost estimates for a long-term strategy to achieve interoperability by enrolling individuals in US-VISIT using more than two fingerprints. In previous correspondence to us, the DOS indicated that its own cost estimates are much higher than the DOJ's. However, as we stated above, the DOS did not include its own cost estimates or provide alternative suggestions. Our reading of the DOJ's proposal indicated that it is not intended to dismantle the DOS's nor the DHS's Biometric Visa and US-VISIT programs. On page 48 of our report, we include a statement from the DOJ's proposal which says that reducing the inconvenience to foreign travelers is one of the benefits of upgrading US-VISIT. If more than two fingerprints are collected from travelers now, they will not have to be re-enrolled in the future.

In response to the DOS's statement that requiring consular officers to collect ten fingerprints would detract from visa interviews and would be detrimental to border security, we believe that conclusion is premature because neither the potential for a ten-fingerprint system to identify more criminal aliens among visitors to the United States, nor the potential additional operational and financial costs of implementing a ten-fingerprint system are known at this point.