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

Follow-up Review of the FBI's Progress Toward Biometric Interoperability Between IAFIS and IDENT

July 2006

I-2006-007

EXECUTIVE SUMMARY

This is the Office of the Inspector General's (OIG) sixth review examining the ability of federal law enforcement and immigration authorities to share automated fingerprint identification information.[1] In this report, we describe the progress since December 2004 toward achieving full interoperability between two automated fingerprint systems: the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS) and the Department of Homeland Security's (DHS) Automated Biometric Identification (IDENT). We also describe the DHS's efforts to make its United States Visitor and Immigrant Status Indicator Technology (US-VISIT) system interoperable with IAFIS. Achieving full interoperability among these systems is intended to provide federal, state, and local law enforcement and immigration officials with direct, real-time access to information in the millions of criminal history and immigration records in IAFIS, IDENT, and US-VISIT.

U.S. 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. The FBI and the former Immigration and Naturalization Service (INS), now part of the DHS, began discussing integrating IAFIS and IDENT in the early 1990s, when the two systems were under development. However, the agencies had a difference of opinion, stemming from the different purposes of their systems, as to the number of fingerprints to collect from apprehended individuals. The FBI created IAFIS to automate its Criminal Master File of 10 rolled fingerprints and serve the needs of the broader law enforcement community.[2] The INS created IDENT using two flat fingerprints to quickly

[1] The previous five reports are: *The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of its IDENT Automated Fingerprint Identification System,* March 2000; *Status of IDENT/IAFIS Integration,* December 2001; *Status of IDENT/IAFIS Integration,* June 2003; *IDENT/IAFIS: The Batres Case and the Status of the Integration Project,* March 2004; and *Follow-up Review of the Status of IDENT/IAFIS Integration,* December 2004. For a description of each report, see the Background and Appendix of the OIG's December 2004 report, available at www.usdoj.gov/oig/reports/plus/e0501/index.htm.

[2] IAFIS contains the largest criminal biometric database in the world, the Criminal Master file, which stores over 50 million fingerprint sets and corresponding criminal history information submitted by federal, state, and local law enforcement agencies. The Criminal Master File records follow the law enforcement standard of taking prints from all 10 fingers by rolling and pressing each finger on either a scanner or a standard paper fingerprint record form (10 rolled prints). Fingerprints also may be taken by pressing fingers straight down (flat fingerprints) and from fewer than 10 fingers.

process large groups of apprehended aliens.[3] Because of the different fingerprint collection methods, the FBI and INS systems could not initially share information. The inability of these immigration and law enforcement fingerprint identification systems to share information prevented law enforcement agencies from identifying fully the criminals and wanted aliens in their custody, and has led to tragic results. In March 2004, the OIG described one such case, in which border authorities twice released a man with an extensive criminal record 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 the man at the border never learned of his criminal record. (See *IDENT/IAFIS: The Batres Case and the Status of the Integration Project,* March 2004.)

In another report, published in December 2004, we found that the differing fingerprint collection requirements of the FBI and the DHS were one of two principal barriers that had created an impasse in achieving full interoperability between IAFIS and IDENT.[4] In that report, we noted that the DHS and the Department of State (DOS), which is responsible for collecting fingerprints from visa applicants, had not agreed to implement the National Institute of Standards and Technology (NIST) recommendation of 10 flat fingerprints as the uniform method for collecting fingerprint information and for searching against large databases.[5] We recommended that the Department report to the President's Homeland Security Council or Congress that it had reached an impasse in interoperability planning and

[3] The DHS subsequently designed US-VISIT to use IDENT to collect two flat fingerprints and a digital photograph from foreign nationals. IDENT contains the fingerprints of over 55 million individuals, including legitimate travelers and immigration violators. According to the DHS, IDENT processes 150,000 to 230,000 daily fingerprint identifications and verifications.

[4] The second principal barrier was that the DHS and the Department of Justice (Department) disagreed on the details of how to make "readily and easily accessible" to federal, state, and local law enforcement agencies the fully interoperable system specified in the USA PATRIOT Act (Patriot Act) and in subsequent congressional legislation.

[5] The NIST Technology Standard, issued in January 2003, calls for 10 flat fingerprints to be collected from foreign nationals and 2 flat fingerprints and a digital photograph to be used to verify a foreign national's identity against an existing enrollment record.

formally request that a decision be made on whether to adopt the NIST Technology Standard.[6]

In our December 2004 report, we also found that the DHS was checking most visitors' fingerprints against an IDENT database supplemented by IAFIS extracts rather than against the full IAFIS database.[7] Checking only a subset of the IAFIS database created a risk that criminal aliens or terrorists could enter the United States undetected, highlighting the need for immigration and law enforcement fingerprint identification systems to share information in order to fully identify the criminals and wanted aliens in their custody. We concluded that for the Department to effectively proceed with making IAFIS interoperable with the biometric fingerprint systems of the DHS, high-level policy decisions needed to be made regarding who should be subjected to fingerprint searches, the fingerprint collection standard to be used, which of the databases should be queried, who should have access to the information, how the information should be used, and who should maintain the databases. In that report, we made five other recommendations to the Department related to the provision of IAFIS extracts to the DHS, risk analysis, sufficiency of IAFIS's capacity for conducting all of the fingerprint searches the DHS requested, upgrades to IAFIS's performance, and IAFIS availability to users of the system.

In this follow-up to our December 2004 report, we examined interoperability planning documents; interagency correspondence; working group agendas; and IAFIS data on capacity, availability, and workload. We also interviewed officials from the Department, DHS, DOS, and NIST, and analyzed data from all four agencies. The scope of this report includes the interoperability progress made from December 2004 through June 2006. Because of the dynamic nature of the project, the details described in this report may change before the project is completed.

RESULTS IN BRIEF

The primary barrier to achieving full interoperability among federal biometric fingerprint systems was resolved in May 2005 when the DHS agreed to use 10 flat fingerprints as the standard for

[6] The Homeland Security Council, under the Executive Office of the President, is responsible for ensuring coordination of all homeland security-related activities among executive departments and agencies.

[7] At that time, the DHS was requesting IAFIS fingerprint searches on less than 1 percent of the visitors subjected to US-VISIT (about 800 per day) at ports of entry.

US-VISIT.[8] In response to that decision, the FBI and the DHS are implementing the first phase of a three-phase plan to make IAFIS and IDENT, including US-VISIT, fully interoperable by December 2009. In the first phase, the agencies plan to deploy a joint automated system for near real-time sharing of certain key immigration and law enforcement data between the FBI and the DHS by September 3, 2006.[9] The data to be shared are the FBI's "Wants and Warrants" records that have fingerprints associated with them and the DHS's "Visa Denial" and "Expedited Removal" records.[10]

In the remaining two phases, the FBI and the DHS plan to expand the data shared to include law enforcement and immigration data in IAFIS, IDENT, and US-VISIT and to allow access to that data by federal, state, and local law enforcement agencies, authorized non-criminal justice agencies, and immigration authorities.[11] By December 2009, IAFIS and IDENT users are expected to be able to submit a single request that searches all fingerprint records maintained by the FBI and the DHS to receive associated criminal history and immigration information about the subject. As of June 2006, FBI officials stated that they are on schedule for achieving full interoperability among IAFIS, IDENT, and US-VISIT by December 2009.

To support full interoperability, the FBI is upgrading IAFIS to process more flat (in lieu of rolled) fingerprint submissions, and the DHS is planning to modernize IDENT and convert US-VISIT from a 2- to a 10-fingerprint

[8] The second barrier that we identified in our December 2004 report has been partially resolved. The DHS has agreed to provide the FBI and other law enforcement agencies with access to immigration data; however, the FBI and the DHS have not finalized a method of providing this access.

[9] According to the FBI, "near real time" means that information will be updated within 24 hours. However, the FBI plans to update this information more quickly after September 2006.

[10] Wants and Warrants are records of individuals with active warrants from the Wanted Persons file of the FBI's National Crime Information Center. Visa Denials are the DOS's "Biometric Visa Application Category 1 Critical Refusals," which are fingerprint records from applicants whose visas were denied because the DOS determined that they posed a substantial risk to the United States. Expedited Removals are records of aliens removed from the United States because they lacked proper documentation or committed fraud when attempting to enter the United States.

[11] Authorized non-criminal justice agencies are those agencies permitted to request criminal background checks for employment, licensing, immigration, credentialing, and volunteer activities.

system. The FBI and the DHS are also working to develop an estimate of interoperability costs; have identified technical, funding, and policy risks to achieving full interoperability; and have developed risk mitigation strategies.

To lessen the risk that criminal aliens or terrorists will enter the United States undetected before a fully interoperable system is available, the FBI has taken interim actions. These include providing daily transmissions of key terrorist records to the DHS, improving overall IAFIS availability and capacity for DHS fingerprint searches, and reducing the response time to DHS requests for checks of aliens' fingerprints. However, Department officials feel that the DHS should initiate a risk analysis to determine how many individuals who are exempt from the US-VISIT requirements have records in IAFIS.

We now discuss in more detail the three-phase interoperability plan, IAFIS and IDENT upgrades and the US-VISIT transition to 10 fingerprints, interoperability cost estimates, interoperability risks, the FBI's interim actions, and the risk analysis.

The FBI and the DHS are implementing the first phase of a three-phase plan for achieving full interoperability.

In May 2005, the DHS Secretary announced that the DHS would adopt a 10-fingerprint collection standard for enrolling visitors into US-VISIT, as recommended by the NIST. This decision resolved the primary barrier to achieving interoperability among the FBI's IAFIS and the DHS's IDENT and US-VISIT. The resolution of this issue allowed the FBI and the DHS to begin planning and implementing a three-phase approach to achieve full interoperability. In May 2005, the FBI, DHS, and DOS formed an Integrated Project Team (IPT) to develop a plan to achieve full interoperability in the following three phases: Interim Interoperability, Initial Operating Capability (IOC), and Full Operating Capability (FOC).

Interim Interoperability

The interim interoperability phase, currently being developed, is scheduled to be implemented by September 3, 2006. This phase uses an interim Data Sharing Model (iDSM), which is intended to enable the FBI and the DHS to directly access read-only copies of certain key law enforcement and immigration data from IAFIS and IDENT in near real time. By replicating the data (described below), the FBI and the DHS will each be able to conduct fingerprint searches against the other agency's records at their respective locations. The replicated files will also provide a 24-hour backup for those shared IAFIS and IDENT records. The FBI's and the DHS's replicated files are expected to initially accommodate up to 1 million records each. According to IPT planning documents, the iDSM will deliver the first interoperable biometric data capability between the FBI and the DHS and is intended to serve as a prototype for full interoperability.

For the iDSM to become operational, the FBI and the DHS must identify the records to be shared and then exchange those records. As of June 2006, the FBI and the DHS had each agreed to share read-only copies of the approximately 800,000 FBI Wants and Warrants records that have fingerprints associated with them, 16,000 DOS Visa Denial records, and 390,000 DHS Expedited Removal records. These three sets of records were identified as being the most useful to support FBI and DHS missions and IAFIS and IDENT users' needs. FBI officials told us that, as of June 2006, the iDSM's development was on schedule and that it is expected to become operational by September 3, 2006.

In addition to developing the iDSM to provide the initial interoperability capability, the FBI has taken steps to improve the records available to the DHS until the iDSM becomes operational. On November 30, 2005, the FBI began expanding the Wants and Warrants records extracted from IAFIS to provide the DHS with all newly issued or updated warrants created after November 2005, including those for U.S. citizens. Prior to November 30, 2005, the DHS had access only to a subset of the Wants and Warrants records that did not include U.S. citizens. The DHS's immediate access to these additional records allows immigration officials to conduct fingerprint searches using more complete and current information.

After September 3, 2006, when the iDSM is expected to become operational, the FBI and the DHS plan to begin using and testing the iDSM by conducting fingerprint searches against the data and tracking the number of fingerprint matches. The FBI plans to enable three agencies to submit fingerprint searches through IAFIS to be run against the DHS's records. The three agencies are the Boston Police Department, the Texas Department of Public Safety, and the U.S. Office of Personnel Management. Those agencies represent state and local law enforcement and a federal agency authorized to conduct fingerprint searches for non-criminal justice purposes. The FBI is planning to divide the initial iDSM search capacity of 1,000 daily fingerprint searches among those three agencies. The DHS is planning to use the iDSM to continue searching visitors' fingerprints against the FBI's Wants and Warrants records; once the iDSM is operational, the DHS will be able to conduct those searches against all Wants and Warrants records that contain fingerprints rather than a subset of the records.

Initial Operating Capability

The IOC development phase is scheduled to last approximately 22 months, beginning on September 4, 2006, and ending in July 2008.[12] At the beginning of the IOC phase, the IPT must choose one of three technical solutions currently under consideration for achieving full interoperability. The three technical solutions are the shared data model, the shared services model, and the base case. Under the shared data model, the FBI and the DHS would independently maintain their own biometric (e.g., fingerprint) and biographic data (e.g., name, date of birth, social security number), but would provide a copy of the fingerprint data to the other agency. The receiving agency would be responsible for searching the data and requesting the associated biographic information when a match is encountered. The shared services model would not utilize copies of the FBI's and the DHS's fingerprint data. Instead, each agency would maintain control over its data by requesting that the other agency perform a fingerprint search and return the associated biographic information. Finally, the base case option refers to a slightly improved version of the operational iDSM, which the FBI stated would encompass the DHS's efforts to modernize IDENT as they occur.

The FBI considers the iDSM to be a prototype of the shared data model because it allows the FBI and the DHS to access copies of each other's fingerprint data located on their own servers. The iDSM also includes a shared services component in that the FBI and the DHS must each request immigration and criminal history data from the agency that owns the data when a fingerprint match is encountered. Although the FBI and the DHS have not made a final decision on the technical solution for full interoperability, they are implementing the iDSM to test the shared data approach.

During the IOC development phase, the FBI and the DHS expect to have access to one another's basic immigration and criminal history information associated with any fingerprint searches that result in a match. Specifically, the FBI and the DHS plan to: (1) expand the data shared between them; (2) establish the initial fingerprint search capacity and storage needed for full interoperability; (3) allow federal, state, and local agencies limited access to immigration data, which includes basic biographic data; and (4) provide immigration authorities full access to criminal history information.

[12] The IPT's plans call for the records in the iDSM to remain available for conducting fingerprint searches throughout the 22-month IOC development phase.

Expanded data sharing. During the IOC development phase, the FBI and the DHS plan to expand the data accessible to each agency beyond the records initially selected for sharing through the iDSM. With IOC, the FBI expects to have access to all biometric records in IDENT, and the DHS expects to have access to all biometric records from the IAFIS Criminal Master File.[13] The method of providing this access will depend on which of the technical solutions (shared data or shared services) the IPT selects.

Fingerprint search capacity and storage. The FBI and the DHS also expect to establish the initial fingerprint search and storage capacity needed for full interoperability during the IOC phase.[14] The FBI plans to conduct up to 1,000 initial fingerprint searches per day of selected criminal arrestees and federal employees in positions of public trust or national security against the DHS's records in the iDSM. By the end of the IOC development phase, the FBI plans to increase those fingerprint searches to approximately 50,000 per day and increase the storage capacity to accommodate all the records that will be in IAFIS and IDENT by fiscal year (FY) 2009.

Federal, state, and local agencies' limited access to immigration data. During the IOC development phase, the FBI plans to allow any agency – beyond the three pilot agencies – to request a fingerprint search against the DHS's records. The agencies may be federal, state, or local law enforcement or civil agencies conducting non-criminal justice searches. The FBI's current system receives approximately 60,000 search requests per day from all such agencies. Currently, FBI and other law enforcement personnel can obtain immigration data on a foreign national who is a "subject of interest" by submitting the subject's name to the DHS's Law Enforcement Support Center (LESC).[15] During IOC, the LESC will continue to provide support to the FBI. When the FBI finds a match of a subject's fingerprints against IDENT data, it plans to request the associated immigration data from the LESC. However, as of June 2006, FBI officials indicated that the amount and types of immigration data that the LESC would provide had not been determined. The FBI plans to request the data from the LESC by

[13] Information on individuals with protected identities (e.g., individuals seeking asylum or those enrolled in a witness protection program) will not be shared.

[14] If a shared data model or the base case is chosen, then the necessary capacity of the iDSM will have to be determined. If the shared services model is chosen, then the agencies will need to determine the necessary capacity of IAFIS and IDENT.

[15] The LESC – which operates 24 hours a day, 365 days a year – provides federal, state, and local law enforcement agencies with information about foreign nationals they encounter (e.g., immigration status, identity of individuals arrested or under investigation) by researching information available in various databases and criminal history repositories.

submitting an electronic request known as an Immigration Alien Query, to which the LESC will return an automated response. The FBI will then provide that response back to the requesting agency.

Immigration authorities' full access to criminal history data. For criminal justice purposes, the DHS plans to obtain criminal history information through the existing procedure whereby it submits a query to the FBI's National Crime Information Center. For non-criminal justice agencies (e.g., the DOS), the FBI will provide the criminal history information associated with a fingerprint match after it makes a positive identification in IAFIS.

Full Operating Capability

The FOC phase is scheduled to be developed over 17 months, beginning in July 2008 and ending in December 2009 with full interoperability. During the FOC development phase, the FBI and the DHS plan to: (1) provide complete, standardized data sharing between the FBI and the DHS; (2) increase fingerprint search capacity and storage to accommodate more transactions; and (3) allow federal, state, and local agencies full access to immigration data.

Standardized data sharing. By the end of the FOC development phase, IAFIS and IDENT users are expected to be able to submit a single request that searches all fingerprint records maintained by the FBI and the DHS to receive associated criminal history and immigration information about the subject. The searches are to be based on fingerprints, although interoperability planning documents indicate that expansion to palm prints, facial recognition, and other biometrically based methods may be developed and used by the agencies in the future in a final interoperability solution (beyond FOC). The method of providing this information will depend on which of the technical solutions (shared data, shared services, or a base case) the IPT selects.

Increased fingerprint search capacity and storage. FBI officials stated that by the end of the FOC development phase, the federal, state, and local agencies' capacity to search against the DHS's records will increase from the planned IOC capacity of approximately 50,000 transactions per day to approximately 200,000 per day, a level that according to FBI officials, will accommodate all requests. The FBI and the DHS are also planning to increase the storage capacity of the interoperability solution to accommodate all the records that will be in IAFIS and IDENT by FY 2010.

Federal, state, and local agencies' full access to immigration data. By the end of the FOC development phase, the FBI and the DHS are planning to allow all federal, state, and local law enforcement agencies, as well as authorized non-criminal justice agencies, full access to the DHS's immigration data, both benefits- and enforcement-related. However, the two agencies have not yet decided on the parameters of this access and must still make several policy decisions, including how law enforcement officials and authorized non-criminal justice agencies should use and safeguard the immigration data. With FOC, the LESC is expected to provide more comprehensive immigration information associated with fingerprint matches.

To support full interoperability, the FBI and the DHS are upgrading IAFIS and IDENT, and the DHS is preparing to convert US-VISIT to 10 fingerprints.

Concurrent with the IPT's efforts to implement full interoperability, the FBI and the DHS are independently upgrading IAFIS and IDENT to process 10 flat fingerprints. The FBI is implementing its Next Generation Identification (NGI) initiative, which includes the processing of flat fingerprints, and the DHS is planning to modernize IDENT and convert US-VISIT from a 2- to a 10-fingerprint system.

Upgrading IAFIS

The FBI began planning its NGI initiative (originally called Next Generation IAFIS), in early 2004 to provide IAFIS users with quicker and more accurate fingerprint searches and more complete criminal history information. The FBI now plans to implement NGI concurrently with the overall interoperability effort. The interoperability-related portions of NGI include processing an increased volume of flat fingerprints. The FBI currently accepts flat fingerprint submissions from only three entities: the DOS, the American Bankers Association, and the Ohio Bureau of Criminal Identification and Investigation.[16] NGI is also slated to provide several new services, such as a specialized biometric database expected to provide quicker identification of certain criminals and terrorists and improved disposition data associated with criminal history records. According to the FBI, the interoperability-related portions of NGI are tentatively scheduled to be completed by the end of the FOC phase in December 2009, pending the results of a study the FBI is conducting to determine IAFIS user needs.

[16] To handle the volume of flat fingerprint submissions that will result from all visitors being enrolled into US-VISIT (approximately 43 million per year), the FBI has begun upgrading IAFIS search capacity.

Modernizing IDENT

The DHS is planning to modernize IDENT through an effort it refers to as "Unified IDENT" to accept, store, and process 10 fingerprints and improve fingerprint matching accuracy. The DHS also plans to provide more comprehensive individual alien history information, link its various immigration databases, and establish a "person-centric view" that the DHS expects will allow each individual with an immigration history to have only one identity (known as a unique identifier) in the system. Under the person-centric view, the DHS expects that users will be able to submit a single query and receive a consolidated response containing all benefits- and enforcement-related immigration information associated with the individual in question. The DHS is planning to begin modernizing IDENT during the interim interoperability phase and intends to complete the modernization effort during the FOC phase.

Converting US-VISIT to 10 Fingerprints

The DHS and the DOS have begun planning for the transition of US-VISIT from a 2- to a 10-fingerprint enrollment standard during the interim interoperability phase. The DHS and the DOS currently enroll visitors to the United States into US-VISIT using two flat fingerprints and a digital photograph. DOS officials either enroll visitors at visa-issuing consulates before they travel to the United States or DHS officials enroll visitors at ports of entry upon arrival in the United States. When visitors subsequently re-enter the country, their two fingerprints are matched against their own enrolled fingerprints to verify their identity. Once the new US-VISIT enrollment standard is implemented, the DHS and the DOS plan to begin collecting 10 flat fingerprints from visitors using new scanners (described below), but to continue verifying visitors' identities using 2 fingerprints.

To select new fingerprint scanners that will support the US-VISIT transition, the DHS formed a user group with representatives from the FBI, National Institute of Justice, DOS, NIST, and Department of Defense. The user group defined the criteria for fingerprint scanners that are faster, smaller, and more portable than the devices currently being used by the DOS and other agencies for capturing 10 flat fingerprints. The user group found two vendors capable of developing such scanners within 12 months. The user group plans to test and evaluate the scanners, once they become available, during the interim interoperability phase.

The DOS has begun a series of pilot projects to collect 10 flat fingerprints from visa applicants at selected consulates and embassies. The DOS began its first pilot project in San Salvador, El Salvador in April 2006 and is planning additional pilot projects in London, England in July 2006 and in Riyadh, Saudi Arabia in September 2006. To collect the fingerprints during the pilot projects, the DOS plans to use an existing type of 10-print scanner that the FBI certified as being in compliance with IAFIS. Once smaller, lighter scanners are available, the DOS plans to deploy the devices and require 10 flat fingerprint processing at its remaining consulates and embassies during the IOC phase. Because IDENT is not yet prepared to accept 10 fingerprints from the DOS, the DOS plans to continue transmitting 2 fingerprints to IDENT until September 2006, when IDENT is expected to begin accepting 10 fingerprints.

The IPT is estimating interoperability costs for the IOC phase.

The IPT is working on a cost-benefit analysis, which it expects to complete by August 2006, that will estimate the IOC interoperability-related expenses for the FBI, DHS, and DOS to make IAFIS, IDENT, and US-VISIT interoperable.[17] Those expenses will include agency-specific initiatives needed for interoperability, such as a portion of the FBI's NGI, the DHS's IDENT modernization, and the DHS and DOS joint implementation of a 10-fingerprint enrollment standard for US-VISIT. The final cost will depend largely on which of the technical solutions the IPT chooses for full interoperability. FBI officials noted that achieving full interoperability is dependent on the FBI, DHS, and DOS receiving adequate appropriations to cover all interoperability-related expenses.

The FBI has estimated costs for the first two interoperability phases.

Separate from the IPT's cost-benefit analysis for IOC, FBI officials have developed FBI-specific cost estimates for the first two interoperability phases. For FY 2006, the FBI estimated a cost of $7.9 million for the iDSM and $24 million for the first portion of the IOC phase. In its FY 2006 appropriation, the FBI budgeted $18.9 million for interoperability-related expenses, most of which included reprogrammed funding. For FY 2007, the FBI estimated that $33 million will be needed for hardware and software for the IOC phase, and the FBI subsequently requested that amount in the President's FY 2007 budget.

[17] We attempted to obtain an estimate of the total interoperability-related expenses through the FOC phase but FBI officials stated that a total estimate was not available.

The FBI and the DHS have identified technical, funding, and policy risks and have developed mitigation strategies.

We examined whether the FBI and the DHS (through the IPT) have identified potential technical, funding, and policy risks that could delay full interoperability and whether they have developed corresponding mitigation strategies. We found that the IPT has developed risk management plans and mitigation strategies that appear reasonable for the overall interoperability effort. We also found that the FBI developed a risk management plan with mitigation strategies for its portion of the interim interoperability phase (iDSM).[18]

The IPT recognized several broad risks, including that it had limited time to develop, design, and deploy an interoperability solution; that there could be a lack of financial, personnel, or technical resources within participating agencies; that privacy issues may be of concern; and that IAFIS and IDENT users could misuse the data in the interoperable solution. In terms of the iDSM-specific risks, the FBI identified 57, and as of May 3, 2006, 18 were still considered open.[19] The open risks involved areas such as schedule, technology, system reliability, cost, policy, privacy, and security. Among them were:

- Purchase and receipt of iDSM equipment: The FBI recognized that the acquisition process for the hardware and software needed for the iDSM would be lengthy and could significantly delay the deployment schedule of the first interoperability phase. To address this risk, the FBI stated that the purchase of this equipment must be made by June 2006 and the equipment received by July 2006. As of June 27, 2006, FBI officials stated that they were in the process of purchasing the equipment.

- Sufficient resources for the iDSM: The FBI recognized the possibility that insufficient resources could cause the first interoperability phase to fall behind schedule. To address this risk, the FBI stated it would apply Earned Value Management to optimize investment

[18] FBI officials told us that the DHS has also devised risk management plans for its portion of the interoperability risks. However, we did not verify this with the DHS or examine those plans.

[19] The FBI closed a risk if: (1) it took action to mitigate the risk or render the risk moot, (2) it incorporated a specific risk with another one already being addressed, or (3) it determined that the probability of occurrence was low.

planning and control.[20] Officials from both the FBI and the DHS have indicated that while implementation of the three interoperability phases is currently on schedule, delays in receiving necessary funding would push back the December 2009 target completion date for full interoperability. For example, FBI officials stated that if a purchase request is delayed by as little as 45 days, it could cause the FBI to miss a procurement cycle, which would push back each of the interoperability phases.

- Protection of sensitive data to be shared through the iDSM: Because the data to be shared through the iDSM is considered sensitive, the FBI recognized the risk of not protecting this data and stated that owners of the data may need to restrict access. To address this risk, the FBI is working with privacy officials and conducting analyses to determine whether a privacy impact assessment is needed.[21] The FBI also decided to limit the volume of data initially being shared through the iDSM.

Although these interoperability risks and corresponding mitigation strategies appear to be reasonable, the scope of our review did not include a thorough analysis of whether the IPT or the FBI identified all potential risks to the interoperability project and appropriately closed or mitigated those risks. Further, the FBI has not completed risk analysis plans for the remaining two interoperability phases, although FBI officials stated that they have begun identifying potential risks for the IOC and FOC development phases. We therefore encourage the FBI to continue regularly monitoring the overall risks to the project and to develop risk mitigation strategies for the IOC and FOC phases.

The FBI has taken action to lessen the risk of criminal aliens or terrorists entering the United States undetected.

Since our December 2004 report, the FBI has taken several steps to lessen the risk of criminal aliens or terrorists entering the United States undetected. As our previous report recommended, the FBI has increased the transmission of “Known or Suspected Terrorists” records to the DHS

[20] Earned Value Management is a program management technique for estimating the performance of a project in terms of its budget and schedule while taking risk into consideration.

[21] A privacy impact assessment is an analysis of how an agency handles information on individuals to ensure it conforms to applicable privacy laws and policies. The E-Government Act of 2002 requires executive branch agencies to conduct privacy impact assessments when they develop or modify electronic collections of such information.

from monthly to daily (or as available), which allows the DHS to conduct searches of visitors' fingerprints using the most current IAFIS extracts. Similarly, by improving the FBI's IAFIS availability so that users can access the system 99 percent of the time, the FBI has lessened the risk that the DHS could unknowingly release aliens because it could not access IAFIS to determine whether the aliens had criminal records. Also, the FBI increased IAFIS capacity from 8,000 daily fingerprint transactions from the DHS in 2004 to 20,000 daily transactions in 2005, which is more than sufficient to handle the DHS's current average daily workload for criminal checks. In addition, the FBI has significantly improved IAFIS response time and has implemented a "high priority" designation for DHS fingerprint transactions so that criminal aliens or terrorists can be identified more quickly.

No risk analysis has been conducted on the visitors exempt from the US-VISIT requirements.

During our 2004 review, Department officials proposed conducting a study to determine how many individuals whose fingerprints were in IDENT but who were not subjected to fingerprint searches against IAFIS had records in the IAFIS Criminal Master File. This population would have included both visitors subjected to US-VISIT and those exempt from the US-VISIT requirements.[22] The study would have provided the Homeland Security Council with more information to use in making a decision on a uniform fingerprint collection methodology for foreign nationals. Our December 2004 report encouraged the Department to undertake such a study.

However, after the DHS's May 2005 decision to adopt the NIST Technology Standard, and the subsequent progress made toward achieving full interoperability, the Department announced that it was no longer planning to conduct the study. Given that the FBI and the DHS had already begun planning for full interoperability and were preparing to implement the iDSM, the Department stated, "it is less imperative from [the Department's] perspective to conduct the study." Nonetheless, Department officials stated that the study was still needed to assess the risk of unknowingly admitting criminal aliens into the United States, particularly those exempt from US-VISIT, and suggested to the OIG that the DHS conduct the study.

[22] Visitors exempt from US-VISIT (and therefore not subjected to fingerprint searches against IAFIS) 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.

Department officials stated that it would be valuable to know the "hit rate" (i.e., the number of hits against IAFIS records) of individuals exempt from US-VISIT requirements, particularly the Border Crossing Card population. Department officials explained that because these visitors are not screened against IAFIS upon entry to the United States, the DHS does not know how many may have matches in the FBI's database. The DHS could use that information to inform future immigration policy decisions, such as whether to expand the pool of individuals to which US-VISIT applies. Because it is the DHS's responsibility to prevent inadmissible aliens from entering the country, Department officials asserted that the DHS, not the Department, should undertake the study.

During this review, we asked DHS officials whether they intended to conduct a study similar to the one proposed by the Department using US-VISIT or Border Crossing Card data. On March 29, 2006, officials from the US-VISIT office indicated that the need for conducting this study has been "overcome by events" because the DHS has already decided to implement a 10-fingerprint standard for US-VISIT.

We believe that until full interoperability is achieved in December 2009, the DHS's policy of using IAFIS to check the fingerprints of less than 1 percent of the visitors subjected to US-VISIT will continue to create a risk that criminal aliens or terrorists could enter the United States undetected.[23] Once full interoperability is achieved, this risk will be reduced because the visitors subjected to US-VISIT will be checked against the full IAFIS Criminal Master File. However, this risk will not be eliminated because a substantial number of visitors exempt from US-VISIT, such as Border Crossing Card holders, will not have their fingerprints searched against IAFIS.

CONCLUSION

Since our December 2004 report, the FBI and the DHS have made progress toward achieving full interoperability among IAFIS, IDENT, and US-VISIT. The DHS's decision to implement a 10-fingerprint enrollment standard for US-VISIT resolved 1 of the 2 barriers to interoperability that we identified in 2004. Since then, the FBI and the DHS have formed an interoperability working group and have began implementing the first phase of a three-phase plan to make IAFIS, IDENT, and US-VISIT interoperable by December 2009. In the remaining two phases, the agencies plan to facilitate complete sharing of the immigration and law enforcement records in IAFIS

[23] To date, no known terrorists have been identified through the IAFIS extract process, only criminal aliens.

and IDENT among federal, state, and local law enforcement agencies; authorized non-criminal justice agencies; and immigration officials. Although not completed, the decision to begin sharing immigration information with law enforcement officials through the iDSM partially resolves the second barrier that we identified in 2004. To support full interoperability, the FBI and the DHS are upgrading IAFIS and IDENT to process 10 flat fingerprints, and the DHS is preparing to convert US-VISIT to a 10-fingerprint enrollment standard.

The FBI and the DHS stated that they are on schedule for achieving full interoperability by December 2009. The IPT is estimating the interoperability-related costs for the IOC phase and has identified technical, funding, and policy risks to the overall interoperability effort, along with risk mitigation strategies. Until full interoperability is achieved, the FBI has implemented interim actions since December 2004 that lessen the risk of criminal aliens or terrorists entering the United States undetected.

Based on the results of our current review, we believe that the Department and the FBI have implemented actions to address our recommendations from 2004; therefore, we are closing them. However, there are still milestones and outstanding risks that need to be monitored as the interoperability project moves forward toward full interoperability among IAFIS, IDENT, and US-VISIT. For example, the IPT's risk management plan for the iDSM states that the equipment purchase needed to be made by June 2006 and that the equipment must be received by July 2006. The FBI has noted that if a purchase request is delayed by even 45 days, it could cause them to miss a procurement cycle, which would push back each of the interoperability phases. The OIG plans to monitor the progress of the interoperability project, including the achievement of these and other milestones, until full interoperability is achieved.

Officials from the Department (including the FBI), DHS, and DOS provided informal comments on this report. Those comments reflected a general concurrence with the facts presented in this report.

TABLE OF CONTENTS

INTRODUCTION

The Office of the Inspector General (OIG) conducted this follow-up review to examine the Federal Bureau of Investigation's (FBI) progress toward achieving biometric interoperability between its Integrated Automated Fingerprint Identification System (IAFIS) and the Department of Homeland Security's (DHS) Automated Biometric Identification (IDENT). We also describe the DHS's efforts to make its United States Visitor and Immigrant Status Indicator Technology (US-VISIT) system interoperable with IAFIS.

In this report, the term "biometric interoperability" (interoperability) refers to the FBI's and the DHS's ability to exchange fingerprint data through compatible technology in IAFIS, IDENT, and US-VISIT. Full biometric interoperability (full interoperability) is intended to give federal, state, and local law enforcement agencies and immigration officials direct, real-time, multi-directional access to data in IAFIS, IDENT, and US-VISIT.

Once fully interoperable, the systems should provide:

- Immediate identification and verification of aliens with criminal histories and other high-risk individuals, including those in custody;

- Development and enhancement of investigative cases;

- Support for eligibility determinations for admissibility, benefits, and employment of foreign nationals; and

- Ability to use the data for trend and intelligence analyses.

This is our sixth report since 2000 related to the progress of the efforts to integrate IDENT and IAFIS. The previous reports were:

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

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

- *Status of IDENT/IAFIS Integration* (follow-up report), June 2003;

- *IDENT/IAFIS: The Batres Case and the Status of the Integration Project,* March 2004; and

- *Follow-up Review of the Status of IDENT/IAFIS Integration,* December 2004.

For this report, we focused on the current status of the FBI's efforts to achieve biometric interoperability among its IAFIS and the DHS's IDENT and US-VISIT systems; the remaining actions needed to achieve full interoperability; and the interim measures taken by the FBI to lessen the risk that criminal aliens and terrorists could enter the United States undetected. In reviewing the FBI's actions, we also examined the DHS's and the DOS's efforts related to the interoperability project.

BACKGROUND

This Background section describes the IAFIS, IDENT, and US-VISIT systems; past efforts to achieve interoperability among the systems; the key agencies and working groups involved in the efforts to integrate the systems; and the findings from our December 2004 report that examined the status of the IDENT/IAFIS integration project and the disagreements between the Departments of Justice, Homeland Security, and State regarding development of an interoperable system.

Fingerprint Identification Systems

The IAFIS, IDENT, and US-VISIT systems were designed by different agencies to provide fingerprint identification support for different requirements. A description of each system follows.[24]

IAFIS. The FBI developed IAFIS to store digitized fingerprints and criminal history records to assist federal, state, and local law enforcement agencies in identifying criminals. The FBI also built IAFIS to conduct non-criminal justice (civil) fingerprint background checks for employment and license applications and immigration benefits. Deployed in 1999, the IAFIS automated fingerprint identification system is operated by the FBI's Criminal Justice Information Services (CJIS) Division. IAFIS contains the largest criminal biometric database in the world, the Criminal Master File, which stores over 50 million sets of 10 rolled fingerprints and corresponding criminal history information submitted by law enforcement agencies.[25] IAFIS also contains a Civil Subject Index Master File, which stores non-criminal fingerprints (e.g., fingerprints of military, government, or authorized non-government personnel), and an Unsolved Latent File, which contains latent fingerprint images found at crime scenes.

IDENT. The former Immigration and Naturalization Service (INS) developed IDENT to identify and track individuals apprehended for illegally crossing the U.S. border and to identify recidivists (i.e., those apprehended

[24] For a more detailed description and history of each system, see the OIG's December 2004 report, *Follow-up Review of the Status of IDENT/IAFIS Integration*, Background and Appendix I, www.usdoj.gov/oig/reports/plus/e0501/index.htm.

[25] The Criminal Master File records follow the law enforcement standard of taking prints from all 10 fingers by rolling and pressing each finger on either a scanner or a standard paper fingerprint record form (10 rolled prints). Fingerprints also may be taken by pressing fingers straight down (flat fingerprints) and from fewer than 10 fingers.

more than once).[26] Deployed in 1994, IDENT is an automated fingerprint identification system that matches two flat fingerprints from the right and left index fingers of apprehended aliens against similar fingerprint records contained in a database of over 55 million subjects that includes legitimate travelers and immigration violators.[27] Those fingerprint records are organized into distinct enforcement- and immigration-related data bases:[28]

- Lookout database: The Lookout database contains approximately 920,000 unique fingerprint records, as well as photographs and basic information, for aliens who have been previously deported or who have criminal records. The FBI provides the DHS with some of the data by extracting certain categories of records from IAFIS and sending them to IDENT. Those records include:

    - *Known or Suspected Terrorists:* Approximately 31,000 fingerprint records from individuals detained by the U.S. military, the FBI's most wanted terrorists, and records from certain field investigations.

    - *Wants and Warrants:* Approximately 800,000 records of individuals with active warrants from the Wanted Persons file of the FBI's National Crime Information Center.[29] The FBI initially provided only those "Wants and Warrants" records that met the DHS's screening criteria of individuals who are foreign born, have no place of birth listed, or who have had previous encounters with immigration officials documented in IAFIS. However, the FBI now also provides fingerprint records of U.S. citizens with new or recently updated active warrants.

[26] On March 1, 2003, the INS was transferred to the DHS and its operational responsibilities divided among the Bureau of Customs and Border Protection, the Bureau of Immigration and Customs Enforcement, and the Bureau of Citizenship and Immigration Services.

[27] According to the DHS, IDENT processes 150,000 to 230,000 daily fingerprint identifications and verifications.

[28] IDENT also contains an Asylum database of approximately 501,000 fingerprint records entered and used by immigration officers who process asylum claims, and a Border Crossing Card database of approximately 7.5 million fingerprints of Mexican citizens that is used by DOS officials who process Border Crossing Card applications.

[29] The 800,000 Wants and Warrants reflect the number of records that the DHS had received from the FBI as of June 6, 2006. However this number changes regularly due to the addition of new records and the removal of "demoted" records, which are Wants and Warrants that are no longer active.

- Recidivist database: The Recidivist database contains over 8.3 million unique fingerprint records and photographs of aliens who have been previously apprehended. Those records include the following categories:
    - *Apprehensions:* Approximately 7.8 million fingerprint records of previous DHS and legacy INS enforcement actions.
    - *Alerts:* Approximately 658,000 fingerprint records of previous DHS and legacy INS encounters that may require special attention at a subsequent encounter, such as "armed and dangerous" or an officer safety alert. The alerts also include approximately 390,000 "Expedited Removal" records for aliens that have been removed from the United States because they lacked proper documentation or committed fraud when attempting to enter the United States.
    - *Previous Criminal History:* Approximately 446,000 fingerprint records of individuals from 25 high-risk countries, such as Iraq, Iran, Syria, and Sudan. The FBI provided these records as a one-time transfer and included demoted Wants and Warrants records.

US-VISIT. The DHS developed US-VISIT as an entry/exit tracking system to collect, maintain, and share information on foreign nationals (visitors) in the United States so that immigration officials can determine whether these individuals should be prohibited from entering the country, have overstayed or violated the terms of their admission, or should be detained for law enforcement action. Deployed in January 2004, US-VISIT uses IDENT to collect two flat fingerprints and a digital photograph to provide the biometric identification for visitors. The fingerprints are taken either at ports of entry when the visitors arrive or by Department of State (DOS) employees at visa-issuing consulates before the visitors arrive. The first time a visitor's fingerprints are taken, they are checked against the US-VISIT Watch List database (a "one-to-many" comparison) and enrolled into the US-VISIT Enrollment database by the DHS (at ports of entry) or the DOS (at consulates).[30] The US-VISIT Watch List and Enrollment databases contain the following records from IDENT:

[30] When visitors subsequently enter the United States, their fingerprints are matched only against their own enrolled fingerprints (a "one-to-one" comparison) to verify the visitors' identity.

- US-VISIT Watch List database: The US-VISIT Watch List contains approximately 1.7 million unique fingerprint records of aliens who have been previously deported, previously apprehended, or who have been denied a visa. Those records include the entire Lookout database, plus:

    - The previous criminal history records (in the Recidivist database),

    - The Expedited Removal records (in the Recidivist database), and

    - "Visa Denial" records, formally called "Biometric Visa Application Category 1 Critical Refusals," constituting approximately 16,000 fingerprint records from applicants whose visas were denied because the DOS determined that they posed a substantial risk to the United States.[31]

- US-VISIT Enrollment database: The US-VISIT Enrollment database contains over 43 million unique fingerprint records of foreign nationals who have visited the United States or applied for an immigration benefit, such as a visa or a Border Crossing Card. According to the DHS, the US-VISIT Enrollment database has been increasing by approximately 80,000 fingerprint records per day since 2004.

Interoperability of Fingerprint Identification Systems

IAFIS and IDENT were not designed to be interoperable.

The FBI and the INS began discussing integrating IAFIS and IDENT in the early 1990s when the two systems were in their development stages. However, the agencies had a difference of opinion, stemming from the different purposes of the systems, as to whether the INS should collect 2 or 10 fingerprints from apprehended aliens. The FBI created IAFIS to automate its Criminal Master File and serve the needs of the law enforcement community. Because fingerprints at crime scenes may be from any finger, the law enforcement standard requires that officers take prints from all 10 fingers of a subject. Conversely, the INS created IDENT as an internal system to track aliens apprehended illegally crossing the border

[31] Although visitors' fingerprints are compared to those on the Watch List, they are not searched against IDENT's Apprehension, Asylum, or Border Crossing Card databases. However, DHS officials have informed us that by the end of fiscal year (FY) 2006, all IDENT databases will be searched during the US-VISIT process.

between ports of entry and to subsequently identify those who illegally crossed the border more than once. Because the INS frequently apprehended large groups of aliens that had to be processed quickly, taking 10 rolled fingerprints was deemed too time-consuming, and IDENT therefore was designed to use only 2 fingerprints.

Congress directed that fingerprint identification systems be interoperable.

Since the late 1990s, Congress has expressed concern that IAFIS and IDENT could not share data readily. After the terrorist attacks of September 11, 2001, Congress required that federal fingerprint identification systems be made interoperable so that aliens and visitors to the United States who are criminals or known or suspected terrorists can be more readily identified.

In the 2001 USA PATRIOT Act (Patriot Act), Congress required 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 . . . ."[32] The Patriot Act specified that this system be "readily and easily accessible" to all consulates, federal inspection agents, and law enforcement and intelligence officers responsible for investigating aliens.

In the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), which amended several provisions of the Patriot Act, Congress changed the description of the electronic system from integrated to interoperable. The Border Security Act, in its description of an "interoperable data system," required that immigration authorities have "current and immediate" access to information in federal law enforcement agencies' databases to determine whether to allow aliens to enter the United States.[33]

Congress directed that the NIST develop a technology standard for interoperability.

One of the requirements in the 2001 Patriot Act was for the Attorney General and the Secretary of State, working jointly with the National Institute of Standards and Technology (NIST), to develop a technology

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

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

standard for verifying the identity of foreign nationals when they apply for visas at U.S. consulates and when they arrive at ports of entry.[34] In response to this requirement, the NIST issued a Technology Standard in January 2003 for collecting fingerprints from foreign nationals. The NIST Technology Standard called for 10 flat fingerprints to be collected for initial enrollment into automated systems and for 2 flat fingerprints and a digital photograph to be used to verify an individual's identity against an existing enrollment record.

US-VISIT did not incorporate the NIST Technology Standard.

Notwithstanding the NIST's January 2003 recommendation of 10 flat fingerprints as the Technology Standard for enrolling individuals in automated systems, on July 18, 2003, the Homeland Security Council Deputies Committee approved US-VISIT's use of 2 flat fingerprints and a photograph to enroll individuals during the system's initial deployment at sea and air ports of entry.[35] In September 2003, the DOS began deploying single-finger scanners at its consulates to prepare for the enrollment of visa applicants into US-VISIT. On January 5, 2004, the DHS launched US-VISIT at air and sea ports of entry.[36]

Integrated IDENT/IAFIS Workstations

In 2004, the DHS began deploying integrated IDENT/IAFIS workstations that allow DHS personnel to directly search IAFIS using 10 rolled fingerprints, and simultaneously enroll individuals into IDENT using 2 fingerprints.[37] The purpose of the integrated workstations was to provide immigration authorities with access to criminal history information

[34] After the DHS's creation through the Homeland Security Act of 2002, the responsibility for immigration-related issues shifted from the Department of Justice to the DHS.

[35] The Homeland Security Council Deputies Committee, organized under the Executive Office of the President, is responsible for ensuring coordination of all homeland security-related activities among executive departments and agencies.

[36] As of December 30, 2005, US-VISIT was operating at 115 airports, 15 seaports, secondary inspection areas at 154 land ports of entry, and approximately 214 visa-issuing consulates. Secondary inspection refers to designated areas at ports of entry that allow inspectors to conduct additional screening to verify visitors' information without causing delays to other arriving visitors.

[37] On September 21, 2004, the DHS reported that it had deployed IDENT/IAFIS workstations to all 142 Border Patrol stations. The DHS then deployed the workstations to all 284 air, land, and sea ports of entry on December 19, 2005. Integrated workstations have also been deployed at 342 Immigration and Customs Enforcement sites.

in IAFIS. Border Patrol agents use those workstations to check all aliens apprehended crossing the border illegally. In addition, inspectors at ports of entry use the workstations to check a small number of aliens who are referred to secondary inspection and denied admittance into the United States. However, the integrated workstations do not meet the goal of full interoperability because they are not multi-directional; the FBI and other law enforcement agencies do not have direct access to the DHS's IDENT.

When the DHS transmits an alien's fingerprints to IAFIS using the integrated workstations, it uses a transaction referred to as a Ten-Print Rap Sheet (TPRS). TPRS transactions provide a quick response to searches of aliens' fingerprints. When the DHS 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 potential match, IAFIS returns the criminal history file.

Key Agencies and Working Groups

Department of Justice. The Department's Justice Management Division (JMD) has maintained oversight of the integration of IAFIS and IDENT since 1999. The Department's Chief Information Officer (CIO) manages the integration project for the Department and represents the Department in meetings with the DHS and other agencies. The FBI's CJIS Division maintains and operates IAFIS.

Department of Homeland Security. The DHS's Bureau of Customs and Border Protection (CBP) employs Border Patrol agents and inspectors, whose mission includes preventing terrorists and criminal aliens from entering the United States and apprehending individuals attempting to enter the United States illegally. The US-VISIT Program Management Office (US-VISIT office) manages US-VISIT and is responsible for communicating with Department of Justice representatives and participating in interagency meetings. CBP and the US-VISIT office report directly to the DHS Deputy Secretary.

Department of Commerce. Scientists at the Department of Commerce's NIST have been working with the FBI for over 30 years to research, develop, and improve fingerprint-matching procedures. They are currently working with representatives from the Department of Justice, the FBI's CJIS Division, DOS, and DHS in regular interagency meetings and joint studies regarding fingerprint biometrics.

Department of State. The DOS's Bureau of Consular Affairs is responsible for administering laws, formulating regulations, and implementing policies relating to consular services and immigration, including issuing visas (both immigrant and non-immigrant), and passports to U.S. citizens. Representatives from the Bureau of Consular Affairs work with the Department of Justice and the DHS on biometrics issues and participate in the interagency meetings regarding fingerprint identification issues.

Homeland Security Council Deputies Committee. The Homeland Security Council Deputies Committee is responsible for ensuring coordination of all homeland security-related activities among executive departments and agencies. It is the senior sub-Cabinet interagency forum for consideration of policy issues affecting homeland security, including fingerprint biometrics, and comprises officials at the deputy level (or their designees) from the Department of Justice, DHS, DOS, and other agencies. The Deputies have met regularly since January 2004 to discuss security issues, including the interoperability of IAFIS, IDENT, and US-VISIT.

Policy Coordination Committee. Formed in January 2004, the Policy Coordination Committee reports to the Homeland Security Council Deputies on various executive branch issues, including current and future use of the fingerprint data contained in IAFIS, IDENT, and US-VISIT. The Policy Coordination Committee is managed by the Office of Management and Budget, and its participants include representatives from the Department of Justice, DHS, and DOS.

Integrated Project Team. Formed in May 2005, the Integrated Project Team's (IPT) mission is to achieve interoperability of biometric (e.g., fingerprint) information in the databases of the FBI and the DHS, and to share related biographic (e.g., name, date of birth, social security number), criminal history, and immigration information in real time or near real time with each other and federal, state, and local law enforcement agencies.[38] The IPT includes representatives from the CJIS Division, the US-VISIT office, and the DOS, with occasional participation from the NIST and other officials. Within the Department of Justice, the Office of the CIO is responsible for monitoring the IPT and its progress and the CJIS Division is the lead component responsible for system development activities.[39]

[38] According to the FBI, "near real time" means that information will be updated within 24 hours. However, the FBI plans to update this information more quickly after September 2006.

[39] Officials from JMD's Management and Planning Staff stated that they are becoming less involved in guiding interoperability efforts since the formation of the IPT, while the Office of the CIO and the CJIS Division have taken more active roles.

The IPT consists of an Executive Committee and three sub-teams: Business Requirements, which ascertains requirements from interoperability stakeholders and establishes operational consensus; Information Technology, which reviews the stakeholders' requirements and advises the IPT on the most feasible technical solutions and logical approaches to design, development, and implementation; and Strategy and Policy, which ensures that the interoperability plan is consistent with FBI and DHS strategies and policies.

In September 2005, the IPT created two working groups to address different aspects of the interoperability effort. The Unique Identity IPT, led by the DHS, is addressing the modifications needed to enable US-VISIT (via IDENT) to make the transition to a 10-fingerprint enrollment standard.[40] The Interoperability IPT, led by the FBI, is addressing all other issues related to making IAFIS interoperable with the DHS's systems. Officials from the FBI and the DHS participate on both working groups and are responsible for jointly implementing interoperability between IAFIS and IDENT.

December 2004 OIG Report on the Integration of IAFIS and IDENT

In our 2004 review, we reported that efforts to achieve full interoperability had stalled because of two major barriers. The Department, DHS, and DOS still had not agreed on either a uniform method for collecting fingerprint information or on the extent to which federal, state, and local law enforcement agencies are to have access to the DHS's immigration records. We also found that the DHS was using data extracted from IAFIS to supplement IDENT and was checking most visitors' fingerprints against only IAFIS extracts, which created a risk that criminal aliens or terrorists could enter the United States undetected. Regarding the FBI, we found that IAFIS capacity was sufficient to handle the DHS's projected daily workload, but the FBI was not prepared to process a large volume of flat fingerprints from the DHS and was not meeting its IAFIS availability requirement of 99 percent.

The Department, DHS, and DOS did not agree on a fingerprint collection standard.

The first major barrier to achieving interoperability between IAFIS and IDENT that we identified in 2004 was that the Department, DHS, and DOS

[40] According to the IPT's *Concept of Operations* and a US-VISIT official we interviewed, the term "unique identity" refers to the biographic information connected to an individual's unique set of fingerprints.

had not agreed on a standard for collecting fingerprint information from foreign nationals applying at consulates for visas to visit the United States or seeking admission to the United States at ports of entry. The Department endorsed the NIST Technology Standard of 10 flat fingerprints for enrolling visa applicants and visitors in US-VISIT because 10 fingerprints would reduce the number of false positives and offer more options for system design and interoperability.[41] We also reported that the agencies were using various fingerprint collection methodologies:

- Department/FBI: The Department's standard was to collect 10 rolled fingerprints for enrollment in IAFIS, although the Department acknowledged that 2 flat fingerprints could be used by the DHS to subsequently verify aliens' identities by checking the aliens' fingerprints against their own enrolled records.

- DHS: The DHS was collecting two flat fingerprints at ports of entry to enroll visitors into US-VISIT. However, the DHS was also collecting 10 rolled fingerprints (to check against IAFIS) from apprehended aliens at Border Patrol stations and from visitors referred to secondary inspection at ports of entry who were not going to be admitted to the United States.

- DOS: The DOS was collecting two flat fingerprints at U.S. consulates to enroll individuals applying for visas into US-VISIT.

See Appendix I for a table comparing the fingerprint collection methods used by the three agencies.

The Department, DHS, and DOS did not agree on how to provide law enforcement agencies with access to the DHS's immigration records.

The second major barrier to achieving interoperability that we identified in 2004 was that the DHS and the Department disagreed on a method of providing 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. Also, the DHS did not believe that the FBI or other law enforcement agencies should have access to US-VISIT records. The DHS maintained that position for several reasons, including that the information in IDENT is incomplete and could be misinterpreted, and the privacy of visitors enrolled in US-VISIT must be protected. However, the OIG report noted that without direct access to the

[41] False positives occur when the system incorrectly determines that a search fingerprint and a file fingerprint are matches.

DHS's IDENT database, it is more difficult for federal, state, and local law enforcement agencies to identify illegal aliens they encounter.

The DHS used data extracted from IAFIS to supplement IDENT.

In our 2004 review, we described how, because the systems are not interoperable, the FBI is periodically providing the DHS with records extracted from IAFIS to supplement information in the IDENT Lookout database. However, there was some delay between when records are extracted from IAFIS and when they are entered into IDENT. For example, the FBI was providing the Known or Suspected Terrorists records to the DHS approximately once a month.

Further, a Department Metrics Study found some of the extracts to be incomplete and prone to errors, which could allow criminals or terrorists whose data has not been extracted from IAFIS to use falsified identity papers to gain entry into the United States.[42] For example, one of the DHS's selection criteria for referring visitors to secondary inspection relies upon self-reported data (e.g., place of birth), but aliens being arrested may lie about their nationality to avoid deportation. Also, many U.S. citizens have an unknown or foreign place of birth. That selection criteria was particularly problematic for the Wants and Warrants extracts because the records of U.S. citizens may be loaded into the IDENT database, while the records of some non-U.S. citizens and potential criminal aliens are not included. The Metrics Study found that the Wants and Warrants extracts failed to include 22 percent (121 of 541) of criminal aliens with active wants and warrants.

The DHS checked most visitors' fingerprints only against IAFIS extracts.

Our 2004 report also noted that the DHS was planning to limit direct IAFIS fingerprint searches (TPRS transactions) to a small percentage of visitors who are referred to secondary inspection and not admitted to the United States.[43] According to the DHS's workload projections through 2005, only about 800 visitors per day – or 0.7 percent of the total projected visitors required to be enrolled in US-VISIT in 2005 – would be subjected to

[42] JMD, *Cost and Operational Effectiveness Analysis, Second Report to Congress*, August 27, 2004.

[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.

direct IAFIS TPRS searches at ports of entry.[44] The other 99.3 percent of visitors enrolled in US-VISIT would be checked against the US-VISIT Watch List, which contains extracts from IAFIS, but not against the full IAFIS Criminal Master File. We found that the DHS's practice of checking 99.3 percent of the visitors' fingerprints only against the limited data extracted from IAFIS and contained in the US-VISIT Watch List increased the risk of admitting criminal aliens. As the Metrics Study showed, searching individuals directly against IAFIS resulted in a significant increase in the number of criminal aliens identified.

At the time of our 2004 review, the Department was interested in determining the risk posed by not checking all visitors against IAFIS. The Department proposed conducting a study to compare data from US-VISIT and other relevant immigration biometric databases against IAFIS. Also, we noted that while the IAFIS capacity of 20,000 daily TPRS transactions was sufficient to handle the then-projected DHS daily workload, if the DHS made a policy decision to request TPRS transactions on all visitors sent to secondary inspection, the resulting workload could exceed the IAFIS capacity.

The FBI was not prepared to process flat fingerprints from the DHS.

In 2004, we found that the FBI had recognized that it needed to upgrade IAFIS to begin accepting flat fingerprints (in lieu of rolled) for non-criminal justice (civil) purposes, such as in the case of employment and license applications or immigration benefits. At that time, the FBI had received approval from its National Crime Prevention and Privacy Compact Council to accept flat fingerprints, but had not yet begun receiving them.[45] Further, although the FBI planned to begin conducting flat fingerprint searches, it was not prepared to process the large number of searches that would be required if the DHS were to start submitting 10 flat fingerprints from all visitors enrolled into US-VISIT.

[44] Visitors exempt from US-VISIT 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.

[45] The Compact Council governs the use of the Interstate Identification Index system of criminal history record information for non-criminal justice purposes, according to the National Crime Prevention and Privacy Compact Act of 1998. The Interstate Identification Index is a segment of IAFIS that stores textual criminal history information on arrests and dispositions of criminal subjects. In addition, the Compact Council advises the CJIS Advisory Policy Board on civil fingerprint standards.

IAFIS was not meeting its availability requirement.

In our 2004 review, we found that IAFIS was not meeting its availability requirement of being accessible to users 99 percent of the time. We determined that from November 2003 through April 2004, IAFIS was unavailable for a total of 161 hours, resulting in an average monthly availability of 96 percent. As a result, it was possible that some aliens whose criminal records were in IAFIS but not in IDENT would be released and allowed to enter the United States due to the system's unavailability. For example, if IAFIS results are not received within about 10 minutes, which may happen if IAFIS is unavailable, immigration officials must make their decisions on whether to further detain aliens based only on the results of IDENT queries. Consequently, some criminal aliens who would have been identified through IAFIS queries may not be detained.

The OIG made six recommendations in our previous report.

In our December 2004 report, we concluded that for the Department to effectively proceed with making IAFIS interoperable with the fingerprint systems of the DHS and the DOS, high-level policy decisions needed to be made regarding who should be subjected to fingerprint searches, the fingerprint collection standard to be used, the databases to be queried, who should have access to the information, how the information should be used, and who should maintain the databases. We recommended that the Department seek to have the federal government address those decisions in a timely way. We made the following six recommendations to 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 [memorandum of understanding] directed by Congress.[46] 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;

[46] In our March 2004 report, we recommended that the Department work with the DHS to develop and implement a memorandum of understanding to guide integration of IAFIS and IDENT. The Conference Report accompanying the FY 2004 omnibus appropriations legislation also directed the Department to develop such a document with the DHS and other appropriate federal agencies regarding the continued integration of fingerprint systems.

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 10 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.

As described in the Results of the Review section, our current review has found that the Department and the FBI have taken steps that were generally responsive to all of the recommendations we made in our December 2004 report.

PURPOSE, SCOPE, AND METHODOLOGY

Purpose

The OIG conducted this review as a follow-up to our December 2004 report. This review assessed the current status of the FBI's efforts in working with the DHS and other agencies to achieve biometric interoperability among its IAFIS and the DHS's IDENT and US-VISIT systems, and the actions taken by the FBI to implement the recommendations contained in our December 2004 report. Specifically, this review assessed the:

- Progress made by the FBI and the Department in working with the DHS and other agencies toward achieving biometric interoperability among IAFIS, IDENT, and US-VISIT;
- FBI's and the DHS's planned actions for achieving full interoperability; and
- Measures taken by the FBI in the interim, before full interoperability is achieved, to lessen the risk that criminal aliens and terrorists could enter the United States undetected.

Scope

The scope of this review included actions taken by the FBI, DHS, and DOS related to achieving interoperability among IAFIS, IDENT, and US-VISIT; the steps taken by the FBI to implement its plans for a next version of IAFIS that are relevant to achieving interoperability; and the DHS's plans to modify IDENT and US-VISIT to process 10 flat fingerprints.[47] Our fieldwork for this review was completed in June 2006. Because of the dynamic nature of the project, the details described in this report may change before the interoperability project is completed.

Methodology

Our fieldwork consisted of interviews as well as documentation review and analysis.

[47] Because the scope involved issues beyond the Department, including issues within the DHS, we coordinated with the DHS's Office of Inspector General during this review.

Interviews. To understand each agency's perspective and role in establishing biometric interoperability, we interviewed officials from the Department, DHS, DOS, and NIST.

Interviews with Department personnel. From the Office of the Chief Information Officer, we interviewed the Special Assistant to the CIO and two Senior Program Analysts. From the Justice Management Division, we interviewed IDENT/IAFIS Program Managers and the Acting Program Manager for the Joint Automated Booking System Program Management Office. From the National Institute of Justice, we interviewed a Senior Program Manager in the Research and Technology Development Division. From the FBI's CJIS Division, we interviewed the Deputy Assistant Director, Operations Branch; two Section Chiefs; a Unit Chief; Program Managers and other officials from the Next Generation Identification and Biometric Interoperability Program Offices; and a Senior Computer Engineer.

Interviews with DHS personnel. From the US-VISIT Program Management Office, we interviewed the Director, Deputy Director, Chief Information Officer, and several key officials assigned to Mission Operations and the Office of the Chief Strategist. From CBP, we interviewed two Program Managers from the Office of Field Operations and an Assistant Chief from the Office of Border Patrol.

Interviews with DOS personnel. From the DOS, we interviewed the Deputy Assistant Secretary of State for Visa Services and a member of the Office of Information Management and Liaison.

Interviews with NIST personnel. From the NIST's Information Access Division, we interviewed the chief scientist with principal responsibility for biometrics research and two of his colleagues.

Document review. To determine the FBI's progress toward achieving biometric interoperability of IAFIS with IDENT, we reviewed and analyzed numerous documents, including a 2005 status update from the Department to Congress; recent congressional testimony and reports; interoperability performance measures; drafts of several interagency (FBI, DHS, and DOS) planning documents; interagency correspondence and working group agendas; IAFIS data on capacity, availability, and workload; Department and DHS plans for the following: the Next Generation Identification initiative, the interim Data Sharing Model, the Fast Capture Finger/Palm Print program, and the US-VISIT transition to 10 fingerprints; and standard operating procedures for the Offices of Border Patrol and Field Operations.

In May 2005, the FBI and the DHS resolved a disagreement that had existed since the early 1990s regarding a common fingerprint collection methodology. Since then, the agencies have begun implementing a three-phase plan for achieving full interoperability of IAFIS, IDENT, and US-VISIT, a process scheduled for completion in December 2009. In the first phase, already under way, the FBI and DHS plan to deploy a joint automated system for sharing key immigration and law enforcement data by September 2006. The FBI and the DHS must implement the remaining two phases to achieve full interoperability that would enable complete sharing of immigration and law enforcement records among federal, state, and local law enforcement agencies. To facilitate full interoperability, both agencies have begun upgrading their IAFIS and IDENT systems to process 10 flat fingerprints. In addition, the DHS is preparing to convert US-VISIT from a 2-fingerprint to a 10-fingerprint enrollment standard. While the FBI and DHS have made progress toward achieving interoperability of their biometric fingerprint identification systems, the project faces significant technological, funding, and policy challenges to meet the scheduled completion date of December 2009.

The FBI and the DHS are implementing the first phase of a three-phase plan for achieving full interoperability.

In May 2005, the DHS Secretary announced that the DHS would adopt a 10-fingerprint collection standard for enrolling visitors into US-VISIT, as recommended in the NIST Technology Standard. The DHS's decision to modify US-VISIT resolved the first of two major barriers that had created an impasse toward achieving interoperability between IAFIS and IDENT.[48] On May 19, 2005, the DHS sent a memorandum to the Homeland Security Council stating that it would modify the US-VISIT program as soon as practicable to use 10 flat fingerprints for enrollment and 2 flat fingerprints for

[48] The second barrier has been partially resolved. In May 2005, the DHS agreed to provide the FBI and other law enforcement agencies with access to immigration data; however, the two agencies have not finalized procedures to provide this access.

identity verification. The Homeland Security Council concurred with the DHS's decision and stated in a "summary of conclusions" dated June 7, 2005, that "it should be the policy of the United States Government that biometric screening of foreign visitors to the United States be based on a fingerprint standard requiring 10-[finger]print capture at enrollment and 2-[finger]print verification thereafter."

The resolution of the impasse has allowed the FBI and the DHS to begin planning their approach to achieving full interoperability of the fingerprint systems. The FBI and the DHS currently are implementing the first phase of a three-phase plan that is intended to produce a joint, automated system for the reciprocal sharing of key immigration and law enforcement data. Appendix II contains a table showing significant interoperability-related events during 2005.

<u>The FBI and the DHS have formed a working group and established a three-phase plan for achieving full interoperability</u>.

In May 2005, the FBI (through the CJIS Division), DHS (through the US-VISIT office), and DOS formed the IPT to coordinate efforts to achieve full interoperability. The IPT charter sets out guiding principles to serve as the foundation for sharing biometric and related information among the agencies in accordance with each agency's mission.[49] Since its creation, the IPT has produced several key interoperability planning documents, including the *DHS/US-VISIT & DOJ/FBI Interoperability Concept of Operations* and the *DHS/US-VISIT & DOJ/FBI Interoperability Business Requirements.*[50] All issues regarding the interoperability of IAFIS and IDENT are vetted through the IPT and its sub-teams.

The IPT plans to accomplish full interoperability in three phases. A brief description of the capabilities planned for each phase follows, while the

[49] The guiding principles state that each agency has responsibility for its own mission, each agency maintains its own repository of information and must ensure its integrity, and each agency must protect the privacy rights of individuals represented by the information it maintains. IPT members from the FBI and the DHS commented that the guiding principles of the IPT, particularly those related to data ownership, were integral to the agencies' agreeing to share data with each other and with federal, state, and local law enforcement agencies.

[50] The *Interoperability Concept of Operations* provides an overview of the proposed operational changes that would be required to achieve full interoperability (e.g., how law enforcement agencies will access and protect immigration data). The *Interoperability Business Requirements,* which the IPT derived from the *Interoperability Concept of Operations*, identifies the interoperability-related business processes and needs of all stakeholders.

phases themselves are described in more detail later in this report. According to CJIS Division officials who participate on the IPT, the interoperability efforts were on schedule as of June 2006.

- Interim interoperability: The interim interoperability phase, currently being developed, is intended to enable the FBI and the DHS to directly access read-only copies of certain key law enforcement and immigration data from IAFIS and IDENT in near real time. By replicating the data, the FBI and the DHS will each be able to conduct fingerprint searches against the other agency's records at their respective locations. The replicated files will also provide a 24-hour backup for those shared IAFIS and IDENT records. The interim interoperability development phase is scheduled to be completed by September 3, 2006.[51]

- Initial Operating Capability (IOC): The IOC development phase is intended to expand the data shared between the two agencies. By the end of the IOC development phase, plans are for the FBI to have access to all fingerprint images from IDENT, and for the DHS to have access to the entire Criminal Master File from IAFIS. This phase is also intended to provide the initial fingerprint search capacity and storage needed for full interoperability. As of June 2006, the IOC development phase was scheduled to last approximately 22 months, beginning on September 4, 2006, and ending in July 2008.

- Full Operating Capability (FOC): During the FOC development phase, the FBI and the DHS plan to provide all federal, state, and local law enforcement agencies, as well as authorized non-criminal justice agencies, access to immigration data from IDENT.[52] By the end of the FOC development phase, the agencies expect to have increased fingerprint search capacity and storage, improved response time, and additional IAFIS capabilities and services. The FOC phase is scheduled to be developed over 17 months, beginning in July 2008 and ending in December 2009 with full interoperability.

[51] The target completion dates for each phase are from a March 30, 2006, schedule developed by the CJIS Division that stated, "Dates are subject to further analysis and funding."

[52] Authorized non-criminal justice agencies are those agencies permitted to request criminal background checks for employment, licensing, immigration, credentialing, and volunteer activities.

The FBI and the DHS are developing the first phase of the interoperability plan.

For the interim interoperability development phase, the FBI and the DHS established the following objectives: (1) meet both agencies' most urgent requirements for data access; (2) share data in both directions; (3) serve as a prototype of technical concepts for full interoperability; and (4) not detract from achieving full interoperability in terms of cost, schedule, effort, and technical architecture. To meet these objectives, the FBI and the DHS began developing the interim Data Sharing Model (iDSM).[53] According to the *iDSM Project Concept of Operations*, the iDSM will deliver the first interoperable biometric data capability between the DHS and the FBI by allowing both agencies to share read-only copies of selected immigration and law enforcement data.[54] For the iDSM to become operational, the FBI and the DHS must identify the records to be shared and exchange the replicated files containing the selected records.

Data to be shared through the iDSM. In September 2005, the FBI, DHS, and DOS signed a letter of concurrence stipulating the data to be shared among agencies and the terms governing the use, disclosure, and protection of the shared data. As of June 2006, the FBI and the DHS had agreed to exchange read-only copies of records identified as being the most useful to support the other agency's mission and data that would support IAFIS and IDENT users' needs. According to iDSM planning documents, both the FBI and the DHS are responsible for updating the data that they share (e.g., expunging records or substituting records with better quality fingerprint images) through an automated process.

The FBI's data. The FBI is planning to transfer all of the approximately 800,000 IAFIS Wants and Warrants records that have fingerprints associated with them to provide the DHS with access to the complete set of these records.[55] Once the iDSM becomes operational, the

[53] The iDSM represents one of three technical solutions that the IPT is considering for full interoperability. These technical solutions are discussed in the next section of this report.

[54] On April 18, 2006, the IPT finalized an *iDSM Concept of Operations*, which defines user needs and operational concepts for the iDSM and describes the components for which the FBI and the DHS each have responsibility (e.g., development, deployment, operations, and maintenance of the iDSM).

[55] Prior to November 30, 2005, the DHS had access only to a subset of the Wants and Warrants records that did not include U.S. citizens. The FBI was providing the DHS with daily extracts of those Wants and Warrants records that met the DHS's screening (cont.)

DHS should have access to all fingerprint records of subjects with active warrants, including U.S. citizens, and the current daily extract process will be eliminated.[56] According to the *iDSM Concept of Operations*, the DHS's access to the full set of Wants and Warrants records will facilitate better decision-making about an individual's admissibility, eligibility for immigration benefits, or deportability from the United States. Access also will allow the DHS to detain individuals who have outstanding arrest warrants and notify the appropriate law enforcement agency. Once all the Wants and Warrants data is available, IDENT users should be able to submit one transaction and receive the FBI's and the DHS's shared criminal history, biographic, and immigration information on the subject whose fingerprints are being searched. The DHS plans to conduct up to 250,000 fingerprint searches of visitors per day against the Wants and Warrants data.

In addition to developing the iDSM to provide the interim interoperability capability, the FBI also has taken steps to improve the records available to the DHS until the iDSM becomes operational. On November 30, 2005, the FBI began expanding the daily Wants and Warrants records extracted from IAFIS to provide the DHS with all newly issued or updated warrants created after November 2005, including those for U.S. citizens. The FBI provides up to 2,500 of these records to the DHS each day. Although technical limitations restrict the number of daily extracts to IDENT, the expansion is nonetheless increasing the information immediately available to the DHS. The DHS's immediate access to these additional records allows immigration officials to conduct fingerprint searches using more complete and current information.

The DHS's data. The DHS is planning to transfer 2 sets of records from IDENT to the iDSM: the approximately 16,000 Visa Denial and the approximately 390,000 Expedited Removal records.[57] The DHS does not currently provide the FBI – or the over 70,000 federal, state, and local law enforcement agencies that contribute to IAFIS – copies of any immigration data. The agencies chose to include those records in the iDSM because they

criteria of individuals who had an unknown or foreign birthplace and citizenship or who had a prior arrest on immigration charges.

[56] Until full interoperability, the FBI plans to continue sending the DHS other IAFIS data, including the fingerprint records submitted as Known or Suspected Terrorists.

[57] The *iDSM Concept of Operations* states that the DHS is planning to include the Recidivists with Alerts records in the iDSM "as soon as technically feasible."

were viewed as being most useful to law enforcement officials.[58] According to the *iDSM Concept of Operations*, these immigration records will help the FBI and other IAFIS users establish the identity of individuals they encounter, determine whether someone is in the United States illegally, conduct better risk assessments, protect officer safety, and enhance law enforcement agencies' ability to develop comprehensive history and threat profiles. The FBI plans to conduct searches of at least 1,000 fingerprint submissions per day against these DHS records. As of June 2006, the DHS had not begun providing copies of these records to the FBI, but DHS officials told us that they would be able to transfer both sets of records to the iDSM by September 3, 2006.

CJIS Division officials stated that the initial iDSM storage capacity for the FBI's and the DHS's replicated files will accommodate up to 1 million records each. They explained that the FBI and the DHS designed each data storage component to accommodate about twice that amount of records to allow for growth and to prevent the need to immediately upgrade the iDSM.

Status of system development. FBI and DHS officials told us that, as of June 2006, the development of the iDSM was on schedule to become operational on September 4, 2006. CJIS Division officials stated they were in the process of purchasing the hardware and software needed for the storing of the replicated files. According to documents the CJIS Division provided, the hardware and software must be delivered by July 2006 to maintain that schedule.

On September 4, 2006, when the iDSM is expected to be fully populated with copies of the Wants and Warrants, Visa Denial, and Expedited Removal records, the FBI and the DHS plan to begin testing and using the iDSM. Once the iDSM is operational, the FBI plans to enable three agencies to submit fingerprint searches through IAFIS to be run against the DHS's records. The three agencies are the Boston Police Department, the Texas Department of Public Safety, and the U.S. Office of Personnel Management. Those agencies represent state and local law enforcement and a federal agency authorized to conduct fingerprint searches for non-criminal justice purposes. The FBI is planning to divide the initial iDSM search capacity of 1,000 daily fingerprint searches among those three agencies. The FBI and the DHS plan to test the iDSM's effectiveness by tracking the number of fingerprint searches each agency

[58] Some FBI personnel have limited access to US-VISIT and other immigration data via a February 2005 memorandum of understanding with the DHS. The DHS provided this access to allow certain FBI personnel at specified locations where the FBI and the DHS are co-located and co-operational (i.e., through the Joint Terrorism Task Forces) to conduct queries.

performs, the number of hits and positive identifications resulting from those searches, the number of individuals apprehended as a result of the positive identifications, the number of false positives, the transfer and storage of data in the iDSM, and the hardware and software performance.

If successful, the iDSM will be instrumental in establishing the foundation for full interoperability between IAFIS and IDENT. The DHS's access to the full set of Wants and Warrants records will help reduce the risk of unknowingly admitting criminal aliens into the United States, including those claiming to be U.S. citizens. Once all the Wants and Warrants containing fingerprint data are transferred to the iDSM, immigration officials will be able to search visitors' fingerprints against all of these records rather than a subset. Similarly, the FBI's access to the Visa Denial and Expedited Removal records will help identify illegal aliens. The FBI's access to those immigration records is significant because, for the first time, the FBI will be able to search fingerprint records in IAFIS against those in IDENT.

The FBI and the DHS plan to implement the remaining two interoperability phases by December 2009.

To achieve full interoperability, the FBI and the DHS must next complete the final two interoperability phases (IOC and FOC). The IOC development phase is planned to begin on September 4, 2006, and continue through July 2008. The FOC development phase is to begin in July 2008 and end by December 2009 with full interoperability.

<u>During the IOC phase, the FBI and the DHS plan to choose a technical solution, expand data sharing, and broaden access to the data</u>.

At the beginning of the IOC development phase, the FBI and the DHS must decide on one of three technical solutions currently under consideration for full interoperability. The three technical solutions, described below, are referred to as the shared data model, the shared services model, and a base case option.

Shared data. This model involves the FBI and the DHS exchanging, and conducting searches against, read-only copies of each other's fingerprint data. Under the shared data model, the FBI and the DHS would independently maintain their own biometric (fingerprint) and biographic data, but would provide a copy of the fingerprint data to the other agency. The receiving agency would be responsible for searching the data and requesting the associated biographic information when a match is encountered. The replicated data also would provide an offsite, 24-hour backup for IAFIS and IDENT data, which the agencies plan to keep updated in near real time. The iDSM has a shared data component because it allows both agencies to access copies of the same biometric data (e.g., Wants and Warrants, Visa Denials, and Expedited Removals).

Shared services. This model involves the FBI and the DHS each sending fingerprint search transactions directly to the other agency's automated system. The shared services model would not utilize copies of the FBI's and the DHS's fingerprint data. Instead, each agency would maintain control over its data by requesting that the other agency perform a fingerprint search and return the associated biographic information. This model is similar to the current process whereby the DHS sends fingerprint searches (TPRS transactions) directly to IAFIS through the IDENT/IAFIS workstations and requests the criminal history or immigration information associated with any fingerprint matches. The iDSM has a shared services component because it allows both agencies to request biographic and criminal history data from the agency that owns it when a fingerprint match is found.

Base case. Finally, the IPT is also considering a base case option, which refers to a slightly improved version of the operational iDSM. According to the FBI, this would encompass the DHS's efforts to modernize IDENT as they occur.

Although the FBI and the DHS have not made a final decision on the technical solution for full interoperability, they are implementing the iDSM as a prototype to test the shared data approach. CJIS Division officials stated that they are currently working on a cost-benefit analysis to determine the most efficient solution and estimate the necessary costs. The cost-benefit analysis is due to be completed by August 2006. CJIS Division officials stated that after September 3, 2006, when the iDSM is expected to become operational, they will test the technology for 30 to 90 days. The FBI and the DHS plan to make the records in the iDSM available for conducting fingerprint searches throughout the 22-month duration of the IOC development phase. Both agencies plan to track and evaluate the number of fingerprint searches performed against the other agency's records and the number of positive identifications resulting from the searches.

During the IOC phase, the FBI and the DHS expect to have access to one another's basic immigration and criminal history information associated with any fingerprint searches that result in a match. Specifically, the FBI and the DHS plan to: (1) expand the data shared between them; (2) establish the initial fingerprint search capacity and storage needed for full interoperability; (3) allow federal, state, and local agencies limited access to immigration data, which includes basic biographic data; and (4) provide immigration authorities full access to criminal history information.

Expanded data sharing. During the IOC phase, the FBI and the DHS plan to expand the data accessible to each agency beyond the records initially selected for sharing through the iDSM. During the IOC phase, the FBI expects to have access to all biometric records in IDENT, and the DHS expects to have access to all biometric records from the IAFIS Criminal Master File.[59] The method of providing this access will depend on which of the technical solutions (shared data or shared services) the IPT selects (the base case would not provide access to all biometric records in IDENT and IAFIS because it includes only the iDSM records). For example, if the shared data model is chosen, both agencies would exchange copies of additional IAFIS and IDENT data, beyond the records in the iDSM.

Fingerprint search capacity and storage. The FBI and the DHS also expect to establish the initial fingerprint search and storage capacity needed for full interoperability during the IOC phase.[60] The CJIS Division plans to search a subset of its federal, state, and local agencies' IAFIS transactions against the DHS's records. Specifically, the CJIS Division plans to conduct up to 1,000 initial fingerprint searches per day of selected criminal arrestees and federal employees in positions of public trust or national security against the DHS's records in the iDSM. By the end of the IOC development phase, the FBI plans to increase those fingerprint searches to approximately 50,000 per day and increase the storage capacity to accommodate all the records that will be in IAFIS and IDENT by FY 2009.

Federal, state, and local agencies' limited access to immigration data. During the IOC development phase, the FBI plans to allow any agency – beyond the three pilot agencies – to request a fingerprint search against the DHS's records. The agencies may be federal, state, or local law enforcement or civil agencies conducting non-criminal justice searches. The FBI's current system receives approximately 60,000 search requests per day from all such agencies. Currently, FBI and other law enforcement personnel can obtain immigration data on a foreign national who is a "subject of interest" by submitting the subject's name to the DHS's Law Enforcement Support Center (LESC).[61] During IOC, the LESC will continue to provide

[59] Information on individuals with protected identities (e.g., individuals seeking asylum or those enrolled in a witness protection program) will not be shared.

[60] If a shared data model or the base case is chosen, then the necessary capacity of the iDSM will have to be determined. If the shared services model is chosen, then the agencies will need to determine the necessary capacity of IAFIS and IDENT.

[61] The LESC – which operates 24 hours a day, 365 days a year – provides federal, state, and local law enforcement agencies with information about foreign nationals they encounter (e.g., immigration status, identity of individuals arrested or under investigation) by researching information available in various databases and criminal history repositories.

support to the FBI. When the FBI finds a match of a subject's fingerprints against IDENT data, it plans to request the associated immigration data from the LESC. However, as of June 2006, FBI officials indicated that the amount and types of immigration data that the LESC would provide had not been determined. The FBI plans to request the data from the LESC by submitting an electronic request known as an Immigration Alien Query, to which the LESC will return an automated response. The FBI will then provide that response back to the requesting agency. Officials from the CJIS Division and US-VISIT office recently met with LESC representatives to plan for the additional workload. According to the *iDSM Concept of Operations*, the initial submissions to the LESC will not exceed 80 requests per day.

Immigration authorities' full access to criminal history data. For criminal justice purposes, the DHS plans to obtain criminal history information through the existing procedure whereby it submits a query to the FBI's National Crime Information Center. For non-criminal justice agencies (e.g., the DOS), the FBI will provide the criminal history information associated with a fingerprint match after it makes a positive identification in IAFIS.

<u>During the FOC phase, the FBI and the DHS are planning to achieve full interoperability</u>.

The FBI and the DHS plan to begin developing the FOC phase in July 2008, after completion of the IOC phase. The FOC phase is scheduled to be developed over 17 months, ending in December 2009, and is to achieve full interoperability among IAFIS, IDENT, and US-VISIT. According to CJIS Division officials, however, implementing the FOC development phase will be affected by the progress of two separate projects that we discuss later in this report: the CJIS Division's development of a new version of IAFIS and the DHS's modernization of IDENT.

The FOC phase is intended to be an expansion of the IOC phase and is planned to: (1) provide complete, standardized data sharing between the FBI and the DHS; (2) increase fingerprint search capacity and storage to accommodate more transactions; and (3) allow federal, state, and local agencies full access to immigration data.

Standardized data sharing. By the end of the FOC development phase, IAFIS and IDENT users are expected to be able to submit a single request that searches all fingerprint records maintained by the FBI and the DHS to receive associated criminal history and immigration information about the subject. The searches are to be based on fingerprints, although interoperability planning documents indicate that expansion to palm prints, facial recognition, and other biometrically based methods may be developed and used by the agencies in the future in a final interoperability solution (beyond FOC).[62] The method of providing this information will depend on which of the technical solutions (shared data, shared services, or a base case) the IPT selects.

Increased fingerprint search capacity and storage. CJIS Division officials stated that by the end of the FOC phase, the federal, state, and local agencies' capacity to search against the DHS's records will increase from the planned IOC capacity of approximately 50,000 transactions per day to approximately 200,000 per day, a level that according to CJIS Division officials, will accommodate all requests. The FBI and the DHS are also planning to increase the storage capacity of the interoperability solution to accommodate all the records that will be in IAFIS and IDENT by FY 2010.

Federal, state, and local agencies' full access to immigration data. By the end of the FOC development phase in December 2009, the FBI and the DHS are planning to allow all federal, state, and local law enforcement agencies, as well as authorized non-criminal justice agencies, full access to the DHS's immigration data, both benefits- and enforcement-related. However, the two agencies have not yet decided on the parameters of this access and must still make several policy decisions. As of April 2006, officials from the CJIS Division and US-VISIT office were meeting to discuss the following issues:

- The FBI and the DHS must decide on a policy for agencies' use of the immigration data. IDENT does not yet provide an individual's comprehensive immigration records, and the DHS is concerned about the potential for law enforcement officers using incomplete information to apprehend someone that they think is an immigration violator. For example, if an individual apprehended along the border is naturalized 2 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 DHS databases that are available to immigration officers but not to law enforcement agencies querying IDENT. The DHS is working to make

[62] The Department's National Institute of Justice is seeking to develop new fingerprint biometrics technology and also to improve current technology. Its Fast Capture Fingerprint/Palm Print Technology initiative is seeking to develop a device capable of collecting the equivalent of 10 rolled fingerprints in less than 15 seconds to improve the screening requirements for criminal, border, transportation, and employment checks. In September 2005, the National Institute of Justice awarded grants to 3 vendors to begin producing such devices, which will be available for testing within 18 to 24 months.

comprehensive information available through its efforts to modernize IDENT (described in the next section).

- The DHS is responsible for protecting the privacy of its information, particularly information on individuals with records in US-VISIT who are presumed to be visitors with no existing criminal records. Thus, the FBI and the DHS must decide on an appropriate policy to ensure that individuals' privacy is protected once agencies can access immigration data.[63]

With FOC, the LESC is expected to provide more comprehensive immigration information associated with fingerprint matches. As of June 2006, CJIS Division officials stated that although the amount and types of immigration data that the LESC would provide have not been determined, they described the idea of providing an "immigration summary sheet" that would contain a consolidated listing, from every available database, of all immigration information (including biographic) related to the subject.

To support full interoperability, the FBI and the DHS are upgrading IAFIS and IDENT, and the DHS is preparing to convert US-VISIT to 10 fingerprints.

Concurrent with the IPT's efforts to implement full interoperability, the FBI and the DHS are independently upgrading IAFIS and IDENT to process 10 flat fingerprints. The FBI is upgrading IAFIS to process more flat fingerprint submissions through its Next Generation Identification (NGI) initiative, and the DHS is planning to modernize IDENT and convert US-VISIT from a 2- to a 10-fingerprint system.

<u>The FBI is upgrading IAFIS through its NGI initiative</u>.

In early 2004, the FBI began planning the NGI initiative (then called Next Generation IAFIS) to provide IAFIS users with quicker and more accurate fingerprint searches and more complete criminal history information. As described below, the interoperability-related portions of the NGI initiative include the processing of an increased volume of flat

[63] Access to immigration information in the DHS's databases is governed by the Privacy Act of 1974 (5 U.S.C. § 552a, as amended), which contains requirements for agencies that maintain a system of records. The Privacy Act defines a system of records as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." The FBI acknowledged the need to protect the privacy of the data to be shared between IAFIS and IDENT users in its risk management plan, which we discuss in the next section of this report.

fingerprints as well as several new services, including a specialized biometric database and improvements in criminal history data.

To oversee NGI planning and implementation, the CJIS Division created the NGI Program Office on March 15, 2005. On July 1, 2005, the FBI awarded a contract for a study to identify development and implementation strategies, functional and system level requirements, and cost estimates. To identify user needs, a team of contractors and FBI personnel from the NGI Program Office completed over 200 interviews with IAFIS users from federal, state, and local agencies, including the DHS and the DOS. NGI Program Office staff stated that they planned to categorize and prioritize user needs and develop cost estimates for them. The study is slated to be completed by December 2006.

The NGI initiative is scheduled to be implemented concurrently with the overall interoperability effort. CJIS Division officials told us that the interoperability-related portions of NGI are tentatively scheduled to be completed by the end of the FOC development phase in December 2009, pending the results of the study. In FY 2006, the FBI received $16.8 million to support IAFIS hardware and software modernization associated with NGI. The CJIS Division estimated that it would need an additional $74.1 million in FY 2007 funding for further NGI development, however the Department requested $38.1 million in FY 2007 to cover the FBI's NGI-related expenses.

Flat fingerprint processing. In our 2004 review, we found that the CJIS Division was planning to incorporate in its NGI initiative flat fingerprint processing for non-criminal justice purposes, including checking employees' and applicants' backgrounds, issuing licenses, and enrolling foreign nationals into US-VISIT. To ensure that IAFIS would be prepared to handle 10 flat fingerprint submissions from the approximately 43 million annual US-VISIT enrollees, we recommended that the FBI develop options for the eventual upgrade of IAFIS.[64] Since we issued our 2004 report, the FBI has begun accepting flat fingerprint submissions on a limited basis. According to NGI Program Office staff, IAFIS currently processes flat fingerprints from three entities: the DOS, the American Bankers Association, and the Ohio Bureau of Criminal Identification and Investigation. From July 27, 2005, through April 17, 2006, those entities submitted approximately 47,000 search requests.

[64] CJIS Division officials explained that the algorithms in IAFIS were designed to process 10 rolled fingerprint submissions and that searching IAFIS using flat fingerprints requires more processing power than searching using rolled fingerprints.

NGI Program Office staff stated that although conducting searches using flat fingerprints requires more processing power than rolled fingerprints, IAFIS currently can process the number of fingerprint searches it is receiving without affecting response time. However, because searches of US-VISIT enrollees' fingerprints will significantly increase the volume of flat fingerprint submissions, the CJIS Division is in the process of implementing upgrades to the fingerprint search segment of IAFIS and to the system's overall search capacity. IAFIS is currently capable of processing up to 100,000 fingerprint searches a day from all sources, but NGI Program Office staff stated that the CJIS Division plans to expand this capacity to at least 200,000 daily fingerprint searches based upon requirements from IAFIS users from federal, state, and local agencies, including the DHS and the DOS.[65]

In addition, NGI planning documents we reviewed indicated that enhancing IAFIS to process more flat fingerprints will require the FBI to develop two separate initiatives. First, the CJIS Division must ensure efficient searching in IAFIS using 10 flat fingerprints and, second, must develop processes for the acceptance of 2-fingerprint verification requests. NGI Program Office staff confirmed that the IAFIS will have the capability to process both 10 flat fingerprint searches and 2-fingerprint verifications.

Enhanced Terrorist Identification Service (ETIS). The CJIS Division is planning to implement a specialized biometric database that will allow more rapid identification of certain criminals and terrorists. The plans call for the ETIS to be integrated with the National Crime Information Center and to be interoperable with other automated fingerprint identification systems. The CJIS Division plans to implement the ETIS during the FOC development phase as a subsystem of IAFIS.

Disposition improvements for criminal history records. Another NGI initiative planned for the FOC development phase will improve the disposition information on criminal history records from the National Crime Information Center. The disposition provides users with information on the outcome of an arrest, such as whether the individual was convicted or acquitted.

[65] Although the DHS is currently the CJIS Division's only TPRS customer, the planned capacity increase should allow the CJIS Division to process TPRS transactions for other agencies in the future. However, if the IPT chooses a shared data or base case option, the need for TPRS transactions will be eliminated because the DHS will be able to conduct searches of visitors' fingerprints against copies of IAFIS data.

The DHS plans to modernize IDENT.

The DHS is planning to begin modernizing IDENT through an effort it refers to as "Unified IDENT" to accept, store, and process 10 fingerprints and improve fingerprint matching accuracy. Further, according to the DHS's draft *Initial 10-print Transition Plan* (10-Print Plan) dated September 16, 2005*,* the DHS plans to provide more comprehensive individual alien history information, link its various immigration databases, and establish a "person-centric view." According to the 10-Print Plan, the goal of the person-centric view is for each individual with an immigration history to have only one identity across all DHS databases (known as a unique identifier). Under the person-centric view, the DHS expects users to be able to submit a single query and receive a consolidated response containing all biographic and immigration information (both benefits- and enforcement-related) associated with the individual being queried. The CJIS Division's schedule reflects that the DHS is planning to begin modernizing IDENT during the interim interoperability development phase and complete the modernization during the FOC development phase.

When we asked DHS officials whether they were on schedule with the IDENT modernization efforts, they stated that the project is likely to take longer than they anticipated, but that this would not affect the achievement of full interoperability. US-VISIT officials stated that they are currently working with CBP and others to consolidate fingerprint records, but that they must acquire additional fingerprint processing power to support searching of those records. US-VISIT officials stated that their first priority was to prepare the records to be shared through the iDSM, particularly the Expedited Removal records, by ensuring that all the records contain an identifying number and that there are no duplicates. US-VISIT officials confirmed that they plan to complete the IDENT modernization project during the FOC development phase.

The DHS plans to convert US-VISIT to 10 fingerprints.

The DHS and the DOS have begun planning for the transition of US-VISIT from a 2- to a 10-fingerprint enrollment standard during the interim interoperability development phase. The DHS has formed a user group to select a new scanner suitable for capturing 10 flat fingerprints. In April 2006, the DOS began a series of pilot projects to collect 10 flat fingerprints from foreign nationals applying for visas at selected consulates and embassies. The DOS plans to complete those pilot projects and begin deploying 10 flat fingerprint processing at the remaining consulates and embassies during the IOC development phase, according to the CJIS Division's schedule. The DHS plans to begin pilot projects to collect 10 flat fingerprints from foreign nationals at selected ports of entry during the IOC development phase.

The DHS has estimated the costs to implement the US-VISIT transition from 2 to 10 fingerprints for both it and the DOS in FY 2006 and FY 2007. According to the DHS's 10-Print Plan, the US-VISIT transition will cost approximately $281 million for both fiscal years ($240 million in DHS costs and $41 million in DOS costs).[66] In FY 2006, the DHS received $340 million for US-VISIT expenses.[67] In FY 2007, the DHS requested $362 million for US-VISIT expenses.

The DHS's plans to convert US-VISIT. In preparation for modifying US-VISIT, the DHS formed a user group with representatives from the FBI, the National Institute of Justice, the DOS, the NIST, and the Department of Defense. The user group identified a need for fingerprint scanners that are faster, smaller, and more portable than the devices currently being used to capture 10 flat fingerprints.[68] The user group agreed on a set of core requirements and issued a Request for Information to vendors to develop a device capable of capturing 10 flat fingerprints. In a December 2005 report, the user group determined that, while the industry currently does not offer a device that meets all of its core requirements, two vendors would be able to provide, within 12 months, such a device.[69] The DHS plans to test and evaluate the devices during the interim interoperability development phase, according to the CJIS Division's schedule.

The DOS's pilot projects to collect 10 flat fingerprints. In April 2006, the DOS began testing software capable of processing either 2 or 10 fingerprints at the consulate office in Cairo, Egypt. The DOS also began a series of pilot projects recently to collect 10 flat fingerprints from visa

[66] The $281 million represents the higher of 2 cost estimates for the US-VISIT transition that the DHS provided in its 10-Print Plan. The higher estimate assumes that the transition to 10 fingerprints would require modifications to existing ports of entry facilities, whereas the lower estimate assumes that the transition would not require modifications.

[67] The DHS's FY 2006 budget request included $24 million to begin implementing the person-centric view.

[68] Current scanners used by the DOS and other agencies are capable of capturing 10 flat fingerprints. However, according to the user group, those devices are limited in many respects (e.g., fingerprint capture time, scanner size, image quality) and do not offer the capabilities that the DHS and the DOS have identified as necessary for the efficient collection of 10 flat fingerprints from foreign nationals.

[69] Smart Border Alliance, *10 Print Capture RFI Study Report*, December 2005.

applicants at selected consulates and embassies. The DOS began its first pilot project in San Salvador, El Salvador in April 2006 and is planning additional pilot projects in London, England in July 2006 and in Riyadh, Saudi Arabia in September 2006.

According to DOS officials, the pilot projects will test the process of collecting 10 fingerprints in an operational environment to identify the length of time needed to collect the fingerprints, the quality of the fingerprint images collected, and additional training needs. However, because IDENT is not yet prepared to accept 10 fingerprints, the DOS plans to continue transmitting 2 flat fingerprints for searches against IDENT.[70] DOS officials stated that they did not anticipate sending 10 flat fingerprint images to the DHS for inclusion in IDENT until September 2006, when IDENT is expected to begin accepting 10 fingerprints. To collect the fingerprints during the pilot projects, the DOS plans to use an existing type of 10-print scanner that the FBI certified as being in compliance with IAFIS. Once smaller, lighter scanners are available, the DOS plans to deploy the devices and require 10 flat fingerprint processing at its remaining consulates and embassies during the IOC development phase.

Pilot projects to collect 10 flat fingerprints from foreign nationals at selected ports of entry are scheduled to occur during the IOC phase, according to the CJIS Division's schedule. In April 2006, DHS officials stated that the pilot locations had not yet been identified. They also stated that before the DHS decides on appropriate ports of entry for a pilot, they must conduct further planning, such as operational and process modeling, facilities modifications, proposed technical solutions, and environmental planning, and collaborate with CBP and other stakeholders. The DHS is planning to deploy US-VISIT 10-fingerprint capabilities at all ports of entry and consulates by the end of the FOC development phase.

The IPT is estimating interoperability costs for the IOC phase.

The IPT is working on a cost-benefit analysis, which it expects to complete by August 2006, that will estimate the IOC interoperability-related expenses for the FBI, DHS, and DOS to make IAFIS, IDENT, and US-VISIT interoperable.[71] Those expenses will include agency-specific initiatives needed for interoperability, such as a portion of the FBI's NGI, the DHS's

[70] Until the 10-print records can be transferred to IDENT, the DOS is planning to store them in its Consular Consolidated Database, which contains information on visa applicants.

[71] We attempted to obtain an estimate of the total interoperability-related expenses through the FOC phase but FBI officials stated that a total estimate was not available.

IDENT modernization, and the DHS and DOS joint implementation of a 10-fingerprint enrollment standard for US-VISIT. The final cost will depend largely on which of the technical solutions the IPT chooses for full interoperability. FBI officials noted that achieving full interoperability is dependent on the FBI, DHS, and DOS receiving adequate appropriations to cover all interoperability-related expenses.

The FBI has estimated costs for the first two interoperability phases.

Separate from the IPT's cost-benefit analysis for IOC, FBI officials have developed FBI-specific cost estimates for the first two interoperability phases. For FY 2006, the FBI estimated a cost of $7.9 million for the iDSM and $24 million for the first portion of the IOC development phase. In its FY 2006 appropriation, the FBI budgeted $18.9 million for interoperability-related expenses, most of which included reprogrammed funding.[72] For FY 2007, the FBI estimated that $33 million will be needed for hardware and software for the IOC development phase and the FBI subsequently requested that amount in the President's FY 2007 budget.[73]

The FBI and the DHS have identified technical, funding, and policy risks and have developed mitigation strategies.

We examined whether the FBI and the DHS (through the IPT) have identified potential technical, funding, and policy risks that could delay full interoperability and whether they have developed corresponding mitigation strategies. We found that the IPT has developed risk management plans and mitigation strategies that appear reasonable for the overall interoperability effort. We also found that the FBI developed a risk management plan with mitigation strategies for its portion of the interim interoperability development phase (iDSM).[74]

In a November 2005 draft *Interoperability Concept of Operations*, the IPT identified broad risks that must be managed throughout each of the

[72] That figure consists of $15.5 million of reprogrammed funding and $3.4 million from the FY 2005 funding of the FBI's IDENT/IAFIS integrated workstations.

[73] The Department's FY 2007 appropriations had not yet been awarded at the time this report was published.

[74] FBI officials told us that the DHS Unique Identity IPT has also devised risk management plans for its portion of the interoperability risks. However, we did not verify this with the DHS or examine those plans.

interoperability phases.[75] The IPT devised mitigation strategies for those risks and stated that it, along with the DHS and the DOS, would manage the risks and periodically report to the IPT's Executive Committee on the status of the mitigation effort. The broad risks and mitigation strategies in the document we examined included the following:

- Limited time to develop, design, and deploy an interoperability solution: To mitigate this risk, the IPT stated it would develop a plan with targeted milestones and project measurements.

- Lack of financial, personnel, or technical resources within participating agencies: To mitigate this risk, the IPT stated it would provide joint (FBI and DHS) briefings to the Office of Management and Budget, Congress, and other authorizing/funding bodies to ensure that interoperability remains a priority.

- Privacy issues limiting participation or categories of transactions: To mitigate this risk, the IPT stated that its Strategy and Policy sub-team would address all legal and policy issues.

- Misuse of data in interoperable solution: To mitigate this risk, the IPT stated it would devise protections to guard against misuse of data, including recommendations for policies, procedures, and audits.

The FBI identified the iDSM-specific risks in an April 2006 *iDSM Concept of Operation*s. For the specific risks, the FBI identified corresponding mitigation strategies and risk consequences that build on the broader interoperability risks discussed in the previous document. CJIS Division officials stated that they regularly identify and monitor the iDSM risks, and on May 3, 2006, the officials provided documentation showing 18 open risks and 39 risks that they had closed.[76] The open risks involved areas such as schedule, technology, reliability of systems, cost, policy, privacy, and security. Among them were:

- Purchase and receipt of iDSM equipment: The FBI recognized that the acquisition process for the hardware and software needed for the iDSM would be lengthy and could significantly delay the deployment

[75] In the *Interoperability Concept of Operations*, the IPT defined "risk" as a potential event or condition that would be detrimental to the successful implementation and operation of the interoperability effort.

[76] The FBI closed a risk if: (1) it took action to mitigate the risk or render the risk moot, (2) it incorporated a specific risk with another one already being addressed, or (3) it determined the probability of occurrence was low.

schedule of the first interoperability phase. To address this risk, the FBI stated that the purchase of this equipment must be made by June 2006 and the equipment received by July 2006. As of June 27, 2006, FBI officials stated that they were in the process of purchasing the equipment. As a contingency plan in the event that a delay is encountered, the FBI stated that it would identify any similar equipment within the CJIS Division that can be temporarily but immediately utilized.

- <u>Sufficient resources for the iDSM</u>: The FBI recognized the possibility that insufficient resources could cause the first interoperability phase to fall behind schedule. To address this risk, the FBI stated it would apply Earned Value Management to optimize investment planning and control.[77] Officials from both the FBI and the DHS have indicated that while they are currently on schedule, delays in receiving necessary funding would push back the December 2009 target completion date for full interoperability. For example, FBI officials stated that if a purchase request is delayed by as little as 45 days, it could cause the FBI to miss a procurement cycle, which would push back each of the interoperability phases.

- <u>Protection of sensitive data to be shared through the iDSM</u>: Because the data to be shared through the iDSM is considered sensitive, the FBI recognized the risk of not protecting this data and stated that owners of the data may need to restrict access. To address this risk, the FBI is working with privacy officials and conducting analyses to determine whether a privacy impact assessment is needed.[78] The FBI also decided to limit the volume of data initially being shared through the iDSM.

Although the interoperability risks and corresponding mitigation strategies appear to be reasonable, the scope of our review did not include an analysis of whether the IPT or the FBI identified all potential risks to the interoperability project and appropriately closed or mitigated those risks. Further, because the FBI is working toward establishing the iDSM, it has not completed risk analysis plans for the remaining two phases, although

[77] Earned Value Management is a program management technique for estimating the performance of a project in terms of its budget and schedule while taking risk into consideration.

[78] A privacy impact assessment is an analysis of how an agency handles information on individuals to ensure it conforms to applicable privacy laws and policies. The E-Government Act of 2002 requires executive branch agencies to conduct privacy impact assessments when they develop or modify electronic collections of such information.

FBI officials stated that they have begun identifying potential risks for the IOC and FOC development phases. We therefore encourage the FBI to continue regularly monitoring the overall risks to the project and to develop risk mitigation strategies for the IOC and FOC phases.

RESULTS OF THE REVIEW – PART II

The FBI has taken interim actions to lessen the risk of criminal aliens or terrorists entering the United States undetected until full interoperability among IAFIS, IDENT, and US-VISIT can be achieved. For example, the FBI has begun transmitting key terrorist records to the DHS daily instead of monthly. The FBI also has improved fingerprint identification services for the DHS by enhancing IAFIS availability, capacity, and response time.

The FBI has taken action to lessen the risk of criminal aliens or terrorists entering the United States undetected.

Since our December 2004 report, the FBI has taken a series of actions to lessen the risk of criminal aliens or terrorists entering the United States. For example, the FBI has begun implementing the first phase of the IPT's interoperability plan and has initiated improvements to IAFIS. Specifically, the FBI has increased the frequency of its transmissions to the DHS of the Known or Suspected Terrorists records and improved IAFIS availability, as the OIG recommended. The FBI also proactively enhanced IAFIS capacity for processing fingerprint search transactions from the DHS, improved response time for those transactions, and designated the transactions as high priority in IAFIS.

<u>The FBI increased transmissions of Known or Suspected Terrorists records</u>.

In a May 2, 2005, memorandum to the OIG responding to recommendations in our December 2004 report, the Department stated that the FBI had changed its process to provide Known or Suspected Terrorists records to the DHS within 7 days of establishing the record in IAFIS. In a follow-up memorandum to the OIG, the Department stated that the FBI began providing these records on a daily basis on June 24, 2005.

To ensure that the DHS was receiving the Known or Suspected Terrorists extracts on a daily basis, we asked DHS officials whether they had experienced any difficulties in receiving the information. DHS officials responded that they have been receiving the extracts without difficulty, although they commented that they do not always receive the records on a daily basis. To clarify the extracts' frequency of transmission, we asked the Chief of the CJIS Division section responsible for the collection and transmission of the Known or Suspected Terrorists fingerprints why the DHS was not always receiving daily transfers. The Section Chief explained that with the automated extract process, IAFIS communicates with IDENT on a daily basis, but when there are no new records to send, IAFIS does not send extracts.

The FBI has improved IAFIS availability.

In our 2004 review, we found that IAFIS experienced 161 hours of downtime (about 60 percent of it scheduled and 40 percent unscheduled) from November 2003 through April 2004, resulting in an average monthly availability of approximately 96 percent during that period.[79] At that time, CJIS Division officials acknowledged that the downtime exceeded the IAFIS requirement of 99-percent availability. They told us that they were working to limit scheduled downtime to four occasions per year by researching methods of installing faster software, including upgrades that could be accomplished without taking the system out of service.

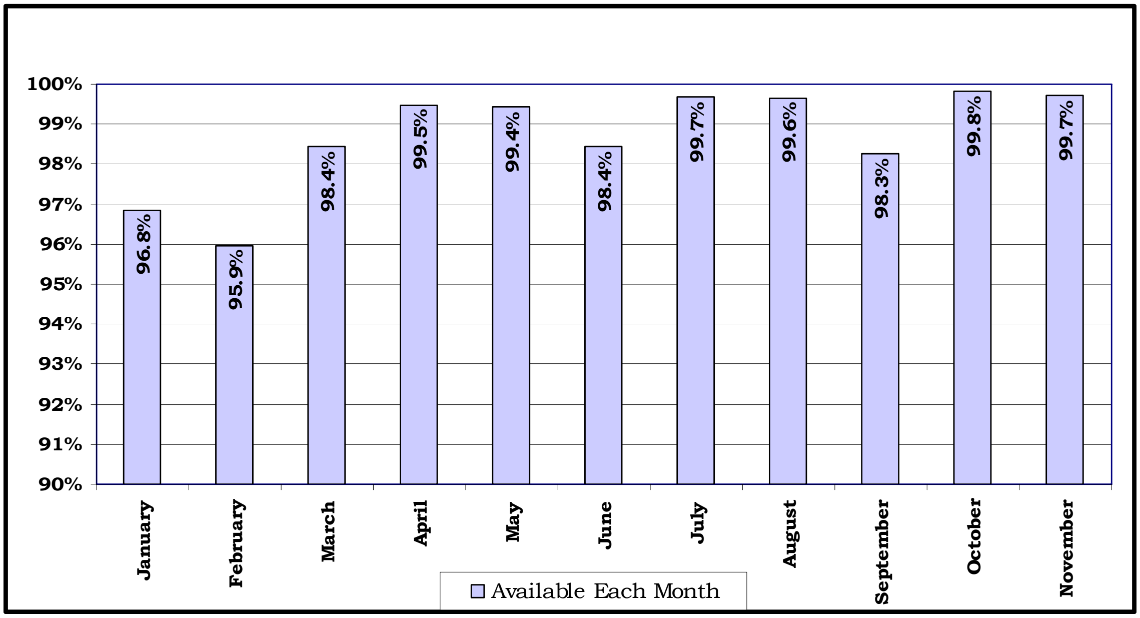
In a series of memorandums responding to our recommendation that the FBI meet its 99-percent availability requirement for IAFIS, the Department described efforts to upgrade the system. In its December 16, 2004, memorandum to the OIG, the Department noted that the FBI had improved availability annually since the system became operational in 1999. The Department reiterated that the CJIS Division was working to reduce unscheduled outages through a series of software and hardware upgrades that would be completed by April 2005. In a May 2, 2005, memorandum, the Department stated that the FBI had completed many of these upgrades, but officials believed it was premature to determine how the upgrades specifically affected IAFIS availability. In an October 6, 2005, memorandum, the Department stated that the FBI's upgrades had improved the overall system availability and that IAFIS was available to users an average of 99.3 percent of the time from May to August 2005. Specifically, the system had 361 minutes of unscheduled downtime and 873 minutes of scheduled downtime (for system maintenance and enhancements).

In our current review, we examined IAFIS availability hours and found that the system was available an average of 98.7 percent of the time from January through November 2005 and that the average availability had risen to 99.3 percent for the period following the series of improvements (May through November 2005). We found that when compared with a similar time period, IAFIS's average availability had increased by 3.1 percent in

[79] Downtime refers to periods when IAFIS is unavailable to users because of planned maintenance (scheduled downtime) or an unexpected service outage (unscheduled downtime). Downtime is significant to the DHS because agents and inspectors process illegal and legal aliens around the clock at Border Patrol stations and ports of entry.

2005.[80] However, when we reviewed the availability on a monthly basis for the period of May through November 2005 (following the IAFIS improvements), we found that June and September fell below the FBI requirement of 99 percent, as shown in Chart 1.

Chart 1: Average IAFIS Availability per Month (January – November 2005)



Source: FBI CJIS Division

When we asked CJIS Division officials about the drop in availability during June and September, they explained that they performed scheduled maintenance during those months in accordance with their quarterly maintenance goals. The CJIS Division coordinates the specific time periods for that maintenance with all IAFIS users, including the DHS, so that downtime will be the least disruptive to their operations.

We found that the CJIS Division has decreased the average number of IAFIS downtime minutes by 80.7 percent – from an average of 1,618 minutes per month from November 2003 through April 2004 to 312 minutes per month from May through November 2005. Additionally, the CJIS Division has decreased the percentage of time IAFIS is down due to unscheduled outages from 40.4 percent for the period covered in our prior

[80] We calculated the percentage change by comparing the 6-month period of November 2003 through April 2004 (the period examined in our prior report) to the 7-month period of May through November 2005. May 2005 is the point at which the CJIS Division upgrades resulted in IAFIS improvements and November 2005 reflects the most recent data that was available during our fieldwork.

report to 28.8 percent for the period May through November 2005. A CJIS Division official stated in February 2006 that the CJIS Division has sustained the 99-percent average IAFIS availability since November 2005.

In addition to responding to our recommendation, the CJIS Division initiated another project to further improve IAFIS availability. In 2005, an FBI contractor began a study to identify areas where overall IAFIS availability can be improved, including improving TPRS processing for the DHS. After the review, the CJIS Division expects the contractor to propose solutions for performing quarterly maintenance without affecting the TPRS services, including performing monthly maintenance activities without (or minimizing) a service outage.

The FBI increased IAFIS capacity.

In our 2004 review, we found the existing IAFIS capacity of 8,000 daily TPRS transactions was sufficient to handle the projected DHS workload increase that would result from deployment of the integrated IDENT/IAFIS workstations. We also reported in 2004 that the CJIS Division was planning to increase IAFIS capacity to 20,000 daily TPRS transactions.[81] We concluded that the current and planned IAFIS capacity was sufficient for the DHS's workload projections through 2005, which assumed that less than 1 percent of the visitors subjected to US-VISIT (about 800 per day) would be subjected to direct IAFIS fingerprint searches at ports of entry.

However, we pointed out in our December 2004 review that DHS inspection policy states that "all subjects who are suspected of being inadmissible to the United States shall be queried through IDENT/IAFIS." Had the DHS checked all visitors referred to secondary inspection against IAFIS, the workload would have exceeded the planned capacity of 20,000 daily TPRS transactions. According to data US-VISIT officials provided in 2004, CBP inspectors referred an average of 22,350 visitors to secondary inspection each day between July 1, 2003, and June 30, 2004.[82] Thus, we

[81] The CJIS Division was also planning to increase IAFIS capacity for another type of transaction. In 2004, the IAFIS capacity for Criminal Answer Required (CAR) bookings was 30,000 per day, which the CJIS Division was planning to increase to 60,000 per day in 2005. CAR bookings occur when an alien is booked at a Border Patrol station or port of entry and the officer transmits a CAR transaction (with the alien's 10 rolled fingerprints) to IAFIS so that the record is enrolled into IAFIS and available to other law enforcement agencies.

[82] During FY 2005, CBP inspectors referred an average of 23,934 visitors to secondary inspection each day.

recommended that the Department coordinate with the DHS to identify the actual capacity needed.

In our current review, we found that the Department had not pursued discussions with the DHS regarding expanding IAFIS capacity beyond the 20,000 daily TPRS transactions.[83] In an October 6, 2005, memorandum to the OIG, the Department stated that it did not anticipate that all visitors referred to secondary inspection would be fingerprinted and checked against IAFIS. Only those thought to be inadmissible were to be checked against IAFIS to determine whether they had a prior criminal history record. Because of the ongoing discussion with the DHS regarding interoperability, the Department stated it was premature to determine whether additional IAFIS capacity was needed. For example, if the FBI and the DHS select a shared data model for full interoperability, meaning that the DHS would be searching copies of IAFIS data, then the issue of IAFIS capacity would be eliminated. Therefore, the CJIS Division officials said they have no current plans to expand IAFIS capacity beyond its current 20,000 TPRS transactions per day.

Although the FBI has no plans to expand IAFIS capacity, the Department responded to our recommendation by identifying the costs associated with increasing IAFIS capacity beyond 20,000 daily TPRS transactions. In its October 6, 2005, memorandum to the OIG, the Department stated that while it and the DHS had not specifically identified the transaction volume that would be generated if all visitors referred to secondary inspection were searched against IAFIS, it estimated a cost of between $3 million to $10 million for each additional increment of 10,000 daily TPRS transactions.

We asked DHS officials about their current plans for submitting TPRS transactions to IAFIS. In these interviews, DHS officials stated that the DHS is not planning to expand the number of visitors in secondary inspection subjected to TPRS transactions or change the pool of visitors subjected to US-VISIT at this time.

We analyzed FY 2005 TPRS transaction data from the CJIS Division to determine whether the current IAFIS capacity is sufficient. We found that in FY 2005, IAFIS processed an average of 4,199 daily TRPS transactions

[83] According to CJIS Division officials, they completed an enhancement of IAFIS to support 20,000 TPRS and 60,000 CAR transactions per day on October 4, 2005. This represents a 150-percent increase over the prior TPRS capacity and a 100-percent increase over the prior CAR capacity.

from the DHS.[84] Therefore, the FBI's IAFIS capacity of 20,000 daily TPRS transactions is more than sufficient to handle the DHS's current average daily workload for criminal checks.

The FBI improved IAFIS response time.

The CJIS Division provides IAFIS responses to law enforcement agencies within 2 hours, but the DHS requires faster response times, particularly at Border Patrol stations that must process large numbers of apprehended aliens. According to CJIS Division documentation, its goal is to provide TPRS responses to the DHS within 2 minutes 90 percent of the time and within 3 minutes 100 percent of the time.

We found that the CJIS Division's IAFIS upgrades increased the percentage of responses returned within 3 minutes since 2004. During the period October through December 2005, IAFIS provided 98.2 percent of the TPRS responses within 3 minutes, compared to 93.7 percent during the same 3-month period in 2004. Even with a 6.1-percent increase in the total number of transactions during the most recent period, IAFIS supplied faster responses for a greater percentage of transactions, especially at the 30-second and 1-minute intervals. For example, as shown in Table 1, there was a 132.6-percent change in the percentage of TPRS transactions processed within 1 minute from FY 2004 to FY 2005. These upgrades allowed IAFIS to provide responses to 88.2 percent of the DHS's fingerprint searches within 1 minute.

Table 1: Percentage of TPRS Transactions Processed by IAFIS Within Specific Intervals

Comparison of time periods:	**IAFIS Processing Intervals**			
October-December	**30 seconds**	**1 minute**	**2 minutes**	**3 minutes**
2004	3.7%	37.9%	88.2%	93.7%
2005	6.2%	88.2%	97.2%	98.2%
Percentage change from 2004 to 2005	68.1%	132.6%	10.2%	4.8%

Source: OIG calculations of CJIS Division data

[84] Of the 4,199 daily TPRS transactions submitted through IAFIS during FY 2005, 685 were requested by inspectors at ports of entry and the remaining 3,514 were submitted by the Border Patrol, according to US-VISIT staff.

The FBI designated TPRS transactions as high priority.

To ensure that all TPRS transactions from the DHS are processed as quickly as possible, the CJIS Division created a new designation for TPRS transactions. The designation, referred to as "high priority," means that IAFIS processes those transactions before other criminal fingerprint search transactions. On December 4, 2005, IAFIS began processing TPRS transactions as high priority.

No risk analysis has been conducted on the visitors exempt from the US-VISIT requirements.

During our 2004 review, Department officials proposed that they conduct a study to determine how many individuals whose fingerprints were in IDENT but who were not subjected to fingerprint searches against IAFIS had records in the IAFIS Criminal Master File. This population would have included both visitors subject to US-VISIT and those exempt from the US-VISIT requirements. The study would have provided the Homeland Security Council with more information to use in making a decision on a uniform fingerprint collection methodology for foreign nationals. Department officials told us that they wanted to obtain statistically valid random samples of data from US-VISIT and other relevant immigration databases in IDENT and search that data against IAFIS. The Department had discussed the possible study with the DHS, but the two agencies had not agreed on the parameters of the study or on the data to be sampled. Our December 2004 report recommended that the Department undertake such a study.

In response to our recommendation, the Department CIO wrote to the Director of the US-VISIT office on March 1, 2005, to request that the DHS provide a sample of approximately 5,000 records from the US-VISIT Enrollment and Border Crossing Card databases for comparison to IAFIS. The CIO also stated in the letter that while the process of extracting data from IAFIS into IDENT had produced valuable results in the short term, Department officials believed that other criminal aliens could be identified and therefore denied admission.[85]

However, after the DHS's May 2005 decision to adopt the NIST Technology Standard, and the subsequent progress made toward achieving interoperability, the Department announced that it was no longer planning to conduct the study. In an October 6, 2005, memorandum from the

[85] To date, no known terrorists have been identified through the IAFIS extract process, only criminal aliens.

Department to the OIG, the Department stated that its primary interest in pursuing the study was to encourage further efforts toward interoperability. Given the fact that the FBI and the DHS had already begun planning for full interoperability and preparing to implement the iDSM, the Department stated, "it is less imperative from [the Department's] perspective to conduct the study."

Nonetheless, Department officials stated that the study was still needed to assess the risk of unknowingly admitting criminal aliens into the United States, particularly those exempt from US-VISIT, and suggested to the OIG that the DHS conduct the study. Officials from the Office of the CIO and the Justice Management Division confirmed that although the Department's interest in conducting the study had lessened, the study was still needed to assess this risk.

Once full interoperability is achieved in December 2009, the DHS will be able to use 10 fingerprints to screen the US-VISIT population against IAFIS or copies of IAFIS data. However, Department officials stated that it would be valuable to know the "hit rate" (i.e., the number of hits against IAFIS records) of individuals exempt from US-VISIT requirements, particularly the Border Crossing Card population. Department officials explained that because these visitors are not screened against IAFIS upon entry to the United States, the DHS does not know how many may have matches in the FBI's database. The DHS could use that information to inform future immigration policy decisions, such as whether to expand the pool of individuals to which US-VISIT applies. Because it is the DHS's responsibility to prevent inadmissible aliens from entering the country, Department officials asserted that the DHS, not the Department, should undertake the study.

We then asked DHS officials whether they intended to conduct a study similar to the one proposed by the Department using US-VISIT or Border Crossing Card data. On March 29, 2006, officials from the US-VISIT office indicated that the need for conducting this study has been "overcome by events" because the DHS has already decided to implement a 10-fingerprint standard for US-VISIT.

We believe that until full interoperability is achieved, the DHS's policy of using IAFIS to check the fingerprints of less than 1 percent of the visitors subjected to US-VISIT will continue to create a risk that criminal aliens or terrorists could enter the United States undetected. Once full interoperability is achieved, this risk will be reduced because the visitors subjected to US-VISIT will be checked against the full Criminal Master File. However, this risk will not be eliminated because a substantial number of visitors exempt from US-VISIT, such as Border Crossing Card holders, will not have their fingerprints searched against IAFIS.

CONCLUSION

Since our December 2004 report, the FBI and the DHS have made progress toward achieving full interoperability among IAFIS, IDENT, and US-VISIT. The DHS's May 2005 decision to implement a 10-fingerprint enrollment standard for US-VISIT resolved the primary barrier to interoperability that we identified in 2004. Since then, the FBI and the DHS have formed an interoperability working group and began implementing the first phase of a three-phase plan to make IAFIS, IDENT, and US-VISIT interoperable by December 2009. FBI officials stated that, as of June 2006, they were on schedule with the interoperability plan.

In the first phase, the agencies plan to deploy the iDSM, a joint automated system for real-time sharing of key immigration and law enforcement data between the FBI and the DHS by September 2006. If successful, the iDSM will deliver the first interoperable biometric data capability between the FBI and the DHS. In the remaining two interoperability phases, the FBI and the DHS plan to enable full sharing of immigration and law enforcement records among federal, state, and local law enforcement agencies, authorized non-criminal justice agencies, and immigration officials. In addition, the decision to begin sharing immigration information with law enforcement officials through the iDSM partially resolves the second barrier that we identified in 2004.

To support full interoperability, the FBI is upgrading IAFIS to process more flat fingerprint submissions and the DHS is planning to modernize IDENT and convert US-VISIT from a 2- to a 10-fingerprint system.

Moreover, the IPT is developing a cost-benefit analysis that is expected to provide an estimate of the interoperability-related expenses for the IOC development phase. The IPT plans to complete that analysis by August 2006. The interoperability-related expenses will include agency-specific initiatives needed for interoperability, such as portions of the FBI's NGI, the DHS's IDENT modernization, and the DHS and DOS joint implementation of a 10-fingerprint enrollment standard for US-VISIT. The final cost will also depend on which of the technical solutions the IPT chooses for full interoperability.

There are significant technological, funding, and policy issues facing the FBI and the DHS if they are to meet the scheduled completion date of December 2009 for full interoperability. We found that the FBI has identified both the broad interoperability risks and the iDSM-specific risks and has devised mitigation strategies that appear to be reasonable. However, the scope of this review did not include a thorough analysis of whether the FBI identified all potential risks to interoperability and appropriately closed or mitigated those risks. Further, although FBI officials stated that they have begun identifying potential risks to the IOC and FOC development phases, they have not completed risk analysis plans for those two phases. We therefore encourage the IPT to continue regularly monitoring the overall risks to interoperability and the iDSM, and to develop similar plans and risk mitigation strategies for the IOC and FOC phases.

The FBI has implemented interim actions since December 2004 to lessen the risk of criminal aliens or terrorists entering the United States undetected until full interoperability can be achieved. Transmitting Known or Suspected Terrorists records to the DHS daily instead of monthly allows the DHS to conduct searches of visitors' fingerprints using the most current IAFIS extracts. Increasing IAFIS availability to 99 percent lessens the risk that the DHS could unknowingly release aliens who, though they have no criminal records in IDENT, do have criminal records in IAFIS. Also, by increasing the IAFIS capacity from 8,000 to 20,000 daily TPRS transactions, the FBI has provided a capacity that is more than sufficient to handle the DHS's current average daily workload for criminal checks. Lastly, the FBI's significant improvement in IAFIS response time and implementation of a high-priority designation for the DHS ensures that criminal aliens or terrorists can be identified as quickly as possible.

However, we believe that until full interoperability is achieved in December 2009, the DHS's policy of using IAFIS to check the fingerprints of less than 1 percent of the visitors subjected to US-VISIT will continue to create a risk that criminal aliens or terrorists could enter the United States undetected. Once full interoperability is achieved, this risk will be reduced because the visitors subjected to US-VISIT will be checked against the full IAFIS Criminal Master File. However, this risk will not be eliminated because a substantial number of visitors exempt from US-VISIT, such as Border Crossing Card holders, will not have their fingerprints searched against IAFIS. Department officials feel that the DHS should initiate a risk analysis to determine the hit rate of these visitors.

Based on the results of our current review, we concluded that the Department and the FBI have implemented actions to address the recommendations we made in our December 2004 report and therefore we are closing them.

Nonetheless, important milestones and outstanding risks must be addressed before full interoperability among the FBI's IAFIS and the DHS's IDENT and US-VISIT is achieved. For example, the FBI's risk management plan for the iDSM states that the equipment purchase must be made by June 2006, and that the equipment must be received by July 2006. The FBI has already noted that if a purchase request is delayed by even 45 days, it could cause them to miss a procurement cycle, which would push back the anticipated completion dates of each of the interoperability phases. The OIG plans to monitor the progress of the interoperability project, including the achievement of these and other milestones.

Officials from the Department (including the FBI), DHS, and DOS provided informal comments on this report. Those comments reflected a general concurrence with the facts presented in this report.

APPENDIX I: COMPARISON OF FINGERPRINT COLLECTION METHODS

Rolled prints of 10 fingers (10 rolled prints)	**Flat-pressed prints of 10 fingers** (10 flat prints)	**Flat-pressed prints of 2 fingers** (2 flat prints)
Used by		
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	**DOJ:** FBI is currently implementing this as the standard for civil enrollments and conducting background checks **DHS:** Not yet used; will become US-VISIT enrollment standard **DOS:** Used on a limited basis through pilot projects at selected consulates **NIST** recommended standard to enroll and search interoperable fingerprint identification systems	**DOJ:** Not used, but accepted for one-to-one verification matches **DHS:** Used to enroll aliens in IDENT database as well as for later searches of this database; Until US-VISIT transition to 10 flat prints, used to enroll visitors at ports of entry in US-VISIT (if not done by DOS) **DOS:** Until US-VISIT transition to 10 flat prints, used to enroll visa applicants at consulates in US-VISIT **NIST** recommended standard for one-to-one verifications only
Pros		
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	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	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)
Cons		
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	More expensive than two flats Could be perceived as more intrusive than two flats Slower IAFIS searches than 10 rolled Provides less information than 10 rolled prints for identifying latent fingerprints	Least accurate, results in most false positive hits and more frequent false 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

APPENDIX II: INTEROPERABILITY EVENTS IN 2005

IAFIS/IDENT/US-VISIT Interoperability Events in 2005	
March	
1	FBI CJIS Division proposes to the DHS an interim interoperability solution involving data sharing in near real time.
14	Department CIO sends letter to Homeland Security Council, transmitting December 2004 OIG report and requesting IAFIS/US-VISIT study.
May	
19	DHS Deputy Secretary sends letter to Homeland Security Council, affirming DHS Secretary's decision to modify US-VISIT to take 10 flat fingerprints for enrollment and 2 flat fingerprints and a photograph for verification.
June	
7	Homeland Security Council concurs with the DHS's decision to modify US-VISIT and concludes that biometric screening of all foreign nationals to the United States will be based on 10 flat fingerprints for enrollment and 2 flat fingerprints and a photograph for verification.
21	FBI, DHS, and DOS sign US-VISIT/DOJ FBI Interoperability Integrated Project Team Charter.
24	FBI begins providing updates of fingerprints of Known or Suspected Terrorists to DHS on a daily basis as an interim interoperability solution.
July	
13	DHS Secretary publicly announces decision to accept NIST biometric standard of 10 flat fingerprints for enrollment and 2 flat fingerprints and a photograph for verification.
September	
16	As part of the Fast Capture Fingerprint/Palm Print initiative, the National Institute of Justice awards grants to 3 vendors to develop devices designed to capture the equivalent of 10 rolled fingerprints in 15 seconds or less.
October	
4	FBI completes enhancement of IAFIS capacity to support up to 20,000 daily TPRS and 60,000 daily CAR transactions from the DHS.
6	JMD provides Congress and OIG with status report on efforts to achieve interoperability among IAFIS, IDENT, and US-VISIT.
November	
30	FBI begins transferring the first set of Wants and Warrants records created after November 2005 to the DHS as part of the iDSM.
December	
4	FBI completes final system enhancements to make TPRS transactions for the DHS high priority in IAFIS.
30	DHS completes deployment of US-VISIT to all ports of entry.

Source: OIG