United States Government Accountability Office

GAO

Report to Congressional Requesters

March 2011

DEFENSE BIOMETRICS

DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies

GAO-11-276

March 2011

DEFENSE BIOMETRICS

DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies

GAO Highlights

Accountability • Integrity • Reliability

Highlights of GAO-11-276, a report to congressional requesters

Why GAO Did This Study

Biometrics technologies that collect and facilitate the sharing of fingerprint records, and other identity data, are important to national security and federal agencies recognize the need to share such information. The Department of Defense (DOD) plans to spend $3.5 billion for fiscal years 2007 to 2015 on biometrics. GAO was asked to examine the extent to which DOD has (1) adopted standards and taken actions to facilitate the collection of biometrics that are interoperable with other key federal agencies, and (2) shares biometric information across key federal agencies. To address these objectives, GAO reviewed documents including those related to standards for collection, storage, and sharing of biometrics; visited selected facilities that analyze and store such information; and interviewed key federal officials.

What GAO Recommends

To improve DOD's ability to collect and share information, GAO recommends that DOD implement processes for updating and testing biometric collection devices to adopted standards; fully define and clarify the roles and responsibilities for all biometric stakeholders; finalize an agreement with the Department of Homeland Security (DHS); and identify its long-term biometric system capability needs. DOD agreed with all of GAO's recommendations.

View GAO-11-276 or key components. For more information, contact Davi M. D'Agostino, (202) 512-5431 or dagostinod@gao.gov

What GAO Found

DOD has adopted a standard for the collection of biometric information to facilitate sharing of that information with other federal agencies. DOD recognized the importance of interoperability and directed adherence to internationally accepted biometric standards. DOD applied adopted standards in some but not all of its collection devices. Specifically, a collection device used primarily by the Army does not meet DOD adopted standards. As a result, DOD is unable to automatically transmit biometric information collected to federal agencies, such as the Federal Bureau of Investigation (FBI). For example, this device is responsible for 13 percent of the records maintained by DOD—the largest number of submissions collected by a handheld device, according to DOD. Further, this constitutes approximately 630,000 DOD biometric records that cannot be searched automatically against FBI's approximately 94 million. DOD has not taken certain actions that would likely improve its adherence to standards, all of which are based on criteria from the Standard for Program Management, the National Science and Technology Council, and the Office of Management and Budget guidance, respectively. First, DOD does not have an effective process, procedure, or timeline for implementing updated standards. Second, DOD does not routinely test at sufficient levels of detail for conformance to these standards. Third, DOD has not fully defined roles and responsibilities specifying accountability needed to ensure its collection devices meet new and updated standards.

DOD is sharing its biometric information and has an agreement to share biometric information with the Department of Justice, which allows for direct connectivity and the automated sharing of biometric information between their biometric systems. DOD's ability to optimize sharing is limited by not having a finalized sharing agreement with DHS, and its capacity to process biometric information. Currently, DOD and DHS do not have a finalized agreement in place to allow direct connectivity between their biometric systems. DOD is working with DHS to develop a memorandum of understanding to share biometric information now scheduled for completion in May 2011; however, without the agreement, it is unclear whether direct connectivity will be established between DOD and DHS, which affects response times to search queries. Further, agencies' biometric systems have varying system capacities based on their mission needs, which affects their ability to similarly process each other's queries for biometric information. As a result, DOD and other agency officials have expressed concern that DOD's biometric system may be unable to meet the search demands from their other biometric systems over the long-term. DOD officials do not believe that they need to match other agencies' biometric system capacities because they do not anticipate receiving the same number of queries given differences in mission. However, the advancements other agencies make in their biometric systems may continue to overwhelm DOD's efforts as it works to identify its long-term biometric system capability needs and associated costs.

Contents

Tables

Figures

Abbreviations

ABIS	Automated Biometric Identification System
BIMA	Biometric Identity Management Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOD EBTS	Department of Defense Electronic Biometric Transmission Specification
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
HIIDE	Handheld Interagency Identity Detection Equipment
IAFIS	Integrated Automated Fingerprint Identification System
IDENT	Automated Biometric Identification System

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 31, 2011

Congressional Requesters

The U.S. government continues in its efforts to positively identify those individuals who may do harm to its citizens, whether discovered at the border, airports, military installations, and during operations around the world, or as a result of criminal investigations. Biometrics technologies that collect and facilitate the sharing of fingerprint records, iris scans, and other data, play an important role as a tool to protect national security, and federal agencies increasingly recognize the need to share terrorism-related biometric information. Challenges to national security arise from multiple sources, which make it difficult, if not impossible, for any single agency to effectively address these new threats alone. In that sense, effective collaboration among multiple agencies and across federal, state, and local governments is critical.

On June 5, 2008, the President issued a new national security directive establishing a governmentwide framework for the sharing of biometric information.[1] This directive requires federal agencies to use compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric information, among other things. In November 2008, as a response to the Presidential directive, the Department of Justice (DOJ) in coordination with the Department of State (State), the Department of Homeland Security (DHS), and the Department of Defense (DOD), among others, developed an action plan to recommend actions and timelines for enhancing the existing identification and screening processes by expanding the use of biometrics.

DOD, DOJ (including the Federal Bureau of Investigation (FBI)), DHS, and State collect biometric information to meet their missions. Prior to the issuance of National Security Presidential Directive-59/Homeland Security Presidential Directive-24, these agencies had established formal and informal arrangements regarding the sharing of information among three major biometric systems: (1) the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which is used for law enforcement

[1]The White House, National Security Presidential Directive/NSPD-59 and Homeland Security Presidential Directive/HSPD-24, *Biometrics for Identification and Screening to Enhance National Security* (Washington, D.C.: June 5, 2008).

purposes; (2) DHS's Automated Biometric Identification System, known as IDENT, which is used by the department in cooperation with its components for several missions and functions including border security, naturalization, and counterterrorism activities, as well as State as part of its visa approval process; and (3) DOD's Automated Biometric Identification System, known as ABIS, which stores biometric information collected on non-U.S. persons.[2] These agencies have implemented policies that use standards to facilitate the sharing of information among the three systems.[3] According to officials at DOD, DHS, and FBI, efforts continue to ensure that biometric information is captured so it can be shared by these three biometric systems, and efforts continue to ensure that National Security Presidential Directive-59/Homeland Security Presidential Directive-24 is implemented. DOD's Biometric Identity Management Agency (BIMA) is responsible for DOD's activities to program, integrate, and synchronize biometric technologies and capabilities, including the operation and maintenance of ABIS. The Handheld Interagency Identity Detection Equipment (HIIDE) is one of several biometric collection devices that feed ABIS with collected biometric information, including that from enemy combatants. According to funding figures provided by DOD, about $3.5 billion has been or will be spent to fund its biometrics programs from fiscal year 2007 through fiscal year 2015. More detailed information on funding for DOD's biometric program appears in appendix II.

We have previously reported on DOD's management of its biometrics activities, its efforts to collect and share biometrics information to support

[2]A more complete definition of biometric systems is found in DOD's Biometrics Glossary. As defined in the Glossary, a biometric system contains multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system. A biometric system is an automated system capable of: (1) capturing a biometric sample for a biometric subject; (2) extracting and processing the biometric data from that sample; (3) storing the extracted information in a database; (4) comparing the biometric data with data contained in one or more references; and (5) deciding how well they match and indicating whether or not an identification or verification of identity has been achieved. A biometric system may be a component of a larger system.

[3]Standards provide rules and guidelines to promote interoperability among various systems and are developed through consensus by Standards Development Organizations, such as the National Institute of Standards and Technology and InterNational Committee for Information Technology Standards.

military activities, and gaps in the interagency information sharing effort.[4] In light of the continued importance of biometrics, and its impact on DOD's and other federal agencies' abilities to protect the homeland, you asked us to examine several matters related to biometrics, including standards and interagency processes for sharing biometric information. Accordingly, our objectives were to assess the extent to which DOD (1) adopted standards and has taken actions to facilitate the collection of biometrics that are interoperable with other key federal agencies and (2) shares biometric information across key federal agencies.

DOD, DOJ, State, and DHS rely on three major federal biometric systems as part of preventing terrorists and criminals from harming national security. Our review, therefore, obtained information from these four agencies, with special focus on DOD. We also confined our review to biometric information related to non-U.S. persons, including enemy combatants, and foreign persons of interest as national security threats as well as persons who are local nationals, third-country nationals or contractors, or coalition forces. In addition, we did not evaluate the technical performance of collection devices used to gather identity information.

To conduct this review, we analyzed Presidential directives related to biometrics information, DOD's biometric capability documents, standards for the collection, storage, and sharing of biometrics issued by standards organizations such as the National Institute for Standards and Technology, and interviewed officials from DOD, DHS, DOJ, and State that collect and share biometric information. We conducted site visits to a selection of facilities that gather, analyze, and store biometric information, including the Army's National Ground Intelligence Center, the Army's Biometric Identity Management Agency, and the FBI's Criminal Justice Information Services complex. We also met with U.S. Central Command and U.S. Special Operations Command officials to obtain their views on how these two combatant commands had operationalized the collection of biometric information. More detailed information on our scope and methodology appears in appendix I.

[4]GAO, *Defense Management: DOD Needs to Establish Clear Goals and Objectives, Guidance, and a Designated Budget to Manage Its Biometric Activities*, GAO-08-1065 (Washington, D.C.: Sept. 26, 2008) and GAO, *Defense Management: DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing*, GAO-09-49 (Washington, D.C.: Oct. 15, 2008).

We conducted this performance audit from December 2009 through March 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The FBI, DHS, and DOD are responsible for managing and maintaining the following major biometric systems:

(1) FBI's Integrated Automated Fingerprint Identification System (IAFIS). Established in July 1999 and managed by the FBI's Criminal Justice Information Services division, IAFIS is a national fingerprint and criminal history system that stores, searches, matches, and shares fingerprints. The FBI is currently in the process of transitioning from IAFIS to the Next Generation Identification system, which will include an expansion to biometrics storage and search capabilities for fingerprints; scars, marks, and tattoos; faces; irises; and palms. The Next Generation Identification system is a multiyear effort with six increments that is expected to be completed by 2014.

(2) DHS's Automated Biometric Identification System (IDENT). Established in 1994 and managed by the United States Visitor and Immigrant Status Indicator Technology program, which falls under the purview of the National Protection and Programs Directorate within DHS, IDENT is used by DHS and State for many purposes including border security, information on persons undergoing naturalization and visa processes, and in the agencies' counterterrorism efforts. IDENT stores, searches, matches, and shares fingerprints.[5] According to DHS officials, the department is beginning to look at the collection of irises and has a goal to begin collecting iris images and facial biometrics by 2013.

(3) DOD's Automated Biometric Identification System (ABIS). Established in July 2004 and managed by the Biometrics Identity Management Agency (BIMA, formerly the Biometric Task Force)—which falls under the purview of the Army—ABIS information is used by DOD to identify and

[5]IDENT also currently stores facial images, but does not have a search and match capability for facial images at this time.

verify non-U.S. persons as friend, foe, or neutral, and to help determine if the individual poses a threat or potential threat to national security. BIMA updated ABIS to the Next Generation ABIS in January 2009, which stores, searches, matches, and shares face, fingerprint, iris, palm, and latent fingerprint biometrics.

Several DOD organizations are involved in the management of the biometrics program and in developing guidance on the collection and sharing of biometric information. In July 2000, Congress designated the Secretary of the Army as the Executive Agent for Defense Biometrics. Subsequently, the Secretary of the Army designated the Director of the Army's Biometrics Task Force as the Executive Manager for Biometrics making this office responsible for developing guidance for collecting and processing biometric information. In March 2010, the Biometric Task Force's name was changed and it became the Biometrics Identity Management Agency. Additionally, DOD appointed the Director, Defense Research and Engineering, as the Principal Staff Assistant for Biometrics. In February 2008, DOD issued a biometrics directive identifying organizational roles and authorities for managing biometrics.[6]

Within DOD, biometric capabilities were initially used in the late 1990s as a tool to protect U.S. forces in Korea, and in Kosovo as an intelligence tool. Since the September 11, 2001, terrorist attacks, DOD's mission has included military operations in both Iraq and Afghanistan—where a biometric system was used to protect U.S. soldiers and allies from an unidentified enemy by screening and vetting non-U.S. persons. DOD collects biometric information from persons seeking access to U.S. installations in Iraq and Afghanistan, detainees, and persons encountered by U.S. forces during military operations. (See fig. 1 below.) In January 2007, DOD issued a memorandum stating that DOD would immediately adopt the practice of sharing unclassified DOD biometric information collected from non-U.S. persons[7] with other U.S. departments and

[6]DOD Directive 8521.01E, *Department of Defense Biometrics* (Feb. 21, 2008).

[7]The January 2007 memorandum defined the term U.S. persons as U.S. citizens and aliens lawfully admitted for permanent residence.

agencies having a counter-terrorism mission.[8] DOD considers the variety of mission-needs for collecting biometric information, such as counterintelligence screening, and detainee management and interrogation, and in business operations, such as base access control to verify Common Access Card credentials, which take place in a combat environment.[9] However, DOD's reasons to collect biometric data continuously change as DOD's role evolves wherever military operations are under way; whether in a desert environment fighting insurgents or on the high-seas fighting piracy.

Figure 1: DOD Collects Biometric Information from Persons Seeking Access to U.S. Installations in Iraq and Afghanistan and Persons Encountered by U.S. Forces during Military Operations

DOD servicemembers collect biometrics from a non-U.S. engineer for access purposes.

DOD servicemembers collect an Iraqi man's biometrics during a mission to prevent smuggling.

DOD servicemembers collect biometrics on volunteers in Iraq for security purposes.

Source: BIMA (photos).

[8]The memorandum states that such unclassified biometric information includes data related to terrorism information defined in the Intelligence Reform and Terrorism Prevention Act (Pub. L. No. 108-458) regarding terrorists, detainees, and those individuals/groups posing a threat to the U.S., but excludes data pertaining to U.S. persons, and any sharing of unclassified biometric information unrelated to terrorism information will be determined based upon relevant law and directives and require, at a minimum, a written memorandum from the requesting agency stating the official need for the records, the intended use of the records, the protections and safeguards that will be afforded the records, and the nature or extent of possible further distribution of the records to other organizations or agencies. Memorandum from Deputy Secretary of Defense on the Sharing of DOD Biometric Data and Associated Unclassified Information from Non-U.S. Persons with Interagency Entities (Jan. 10, 2007).

[9]In 1999, the Deputy Secretary of Defense issued a memorandum directing the implementation of a standard smart-card-based identification system for all active duty military personnel, DOD civilian employees, and eligible contractor personnel, to be called the Common Access Card.

DOD's directive that describes the purpose, scope, policy, and responsibilities for the biometrics program uses terms defined by the National Science and Technology Council Subcommittee on Biometrics Glossary.[10] Included in the list of terms and their respective definitions are the following.

- Collect—capture biometric and related contextual data from an individual, with or without his or her knowledge. Create and transmit a standardized, high-quality biometric file consisting of a biometric sample and contextual data to a data source for matching.
- Match—for the purpose of DOD's Directive on biometrics, the process of accurately identifying or verifying the identity of an individual by comparing a standardized biometric file to an existing source of standardized biometric data. Matching consists of either one to one (verification) or one to many (identification) searches.
- Share—exchange standardized biometric files and match results among approved DOD, interagency, and multinational partners in accordance with applicable law and policy.
- Store—the process of enrolling, maintaining, and updating biometric files to make available standardized, current biometric information on individuals when and where required.

To achieve interoperability, policies and implementation guidance on the collection, storage, and sharing of information should be created to ensure compatible implementation of systems based on standards. Standards are developed by Standards Development Organizations, including the National Institute of Standards and Technology, to provide rules and guidelines to promote interoperability among various systems, including biometric systems. Standards Development Organizations also provide rules and guidelines for testing biometrics and for testing conformance to biometric standards. Standards are generally developed through a consensus process that includes the input of various stakeholders from various sectors such as government, academia, and industry. Federal agencies, such as DOD, adopt standards developed by Standards Development Organizations. For example, DOD used standards recommended by the American National Standards Institute and the National Institute of Standards and Technology as a basis to develop DOD's Electronic Biometric Transmission Specification (DOD EBTS).

[10]DOD Directive 8521.01E, *Department of Defense Biometrics* § 3 (Feb. 21, 2008).

DOD Has Adopted Biometric Collection Standards to Enhance Interoperability, but Taking Certain Actions Could Better Ensure Adherence to Standards

DOD has adopted standards for collection of biometric information to facilitate sharing of that information with other federal agencies. DOD recognized the importance of such interoperability and directed adherence to internationally accepted biometric standards. Moreover, DOD has applied the standards to some of its collection devices. However, DOD has not applied the adopted standards to the Army's primary handheld collection device used in Iraq and Afghanistan. As a result, DOD is unable to automatically transmit information collected by this device, which is about 13 percent of approximately 4.8 million biometric records maintained by DOD, to federal agencies, such as the FBI. Further, DOD has not taken certain actions that would help ensure its collection devices meet new and updated standards. First, DOD does not have an effective process, procedure, or timeline for implementing updated standards. Second, DOD does not routinely test devices at sufficient levels of detail for conformance to these standards. Third, DOD has not fully defined roles and responsibilities that specify accountability needed to ensure its collection devices meet new or updated standards.

DOD Has Adopted Standards to Enhance Interoperability with Other Federal Agencies

DOD adopted a standard—DOD EBTS—to facilitate the collection of biometrics and to enhance interoperability of biometrics collected by DOD with other federal agencies' biometric systems.[11] The first version, DOD EBTS version 1.0, was published on August 19, 2005, and the standard has since been updated three times, with the most recent update, DOD EBTS

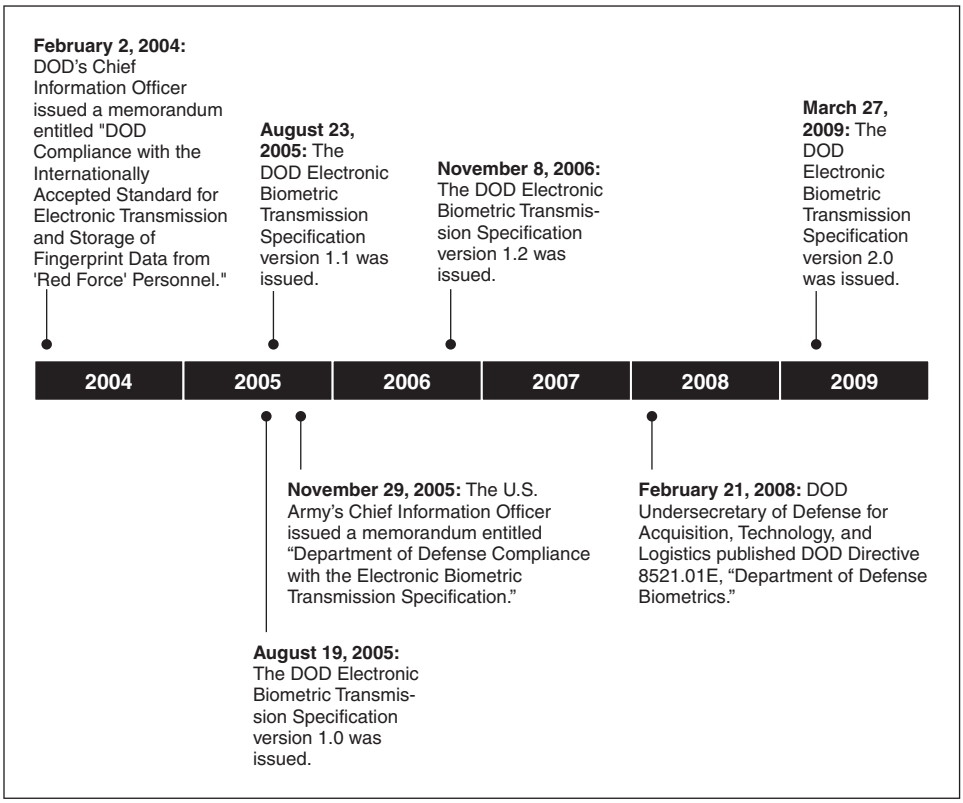
[11]The adoption of standards does not guarantee interoperability, but is an important step in promoting interoperability. According to the Office of Management and Budget (OMB) Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformance Assessment Activities (Washington, D.C.: February 1998), a standard may include a common and repeated use of rules, conditions, guidelines, or characteristics for products, among other things. In addition, a standard may include a specification of dimensions, materials, performance, designs, or operations. DOD Directive 8521.01E, Department of Defense Biometrics (Feb. 21, 2008), states, "Biometric collection, transmission, storage, caching, tagging, and use shall be controlled through the use of DOD-approved national, international, and other consensus-based standards, protocols, best practices, and equipment to ensure consistency and support interoperability."

version 2.0, adopted for use by DOD in April 2010.[12] (See fig. 2 for timeline of DOD's biometric standard.) These DOD standards are based on recommended standards from the American National Standards Institute and the National Institute of Standards and Technology; these standards are also used by the FBI as the basis for its mission-specific requirements.[13] The conformance of biometric collection devices to standards promotes their interoperability with biometric systems within DOD and with other federal agencies, though it does not guarantee interoperability.

[12]The DOD Information Technology Standards Registry is the central repository for DOD-approved information technology standards, including biometric standards. Each standard accepted to the DOD Information Technology Standards Registry is assigned a status as "emerging" or "mandated." "Mandated standards" are mandated for the management, development, and acquisition of new or improving systems throughout DOD. "Information guidance" is also provided in the DOD Information Technology Standards Registry. Updates included DOD EBTS version 1.1 issued on August 23, 2005; DOD EBTS version 1.2 issued on November 8, 2006; and DOD EBTS version 2.0 issued on March 27, 2009. DOD EBTS version 2.0 is currently included in the DOD Information Technology Standards Registry as a "Mandated" standard.

[13]DOD EBTS v.1.1 and v.1.2 were based on ANSI/NIST ITL 1-2000 and EFTS v.7. The most recent, DOD EBTS v. 2.0 is based on ANSI/NIST ITL 1-2007. FBI's requirements include its Electronic Fingerprint Transmission Specification and its Electronic Biometric Transmission Specification.

Figure 2: Timeline of DOD's Biometric Standard



Source: GAO analysis of DOD documents.

Prior to adopting DOD EBTS in 2005, DOD had recognized the importance of interoperability and directed adherence to internationally accepted biometric standards. According to a February 2004 DOD's Chief Information Officer memorandum on DOD compliance with international standards, standardization and interoperability are important for success in fighting terrorism. Success, the memorandum continued, could be enhanced with systems that communicate and share fingerprint data on "red force" personnel, such as detainees, enemy combatants, and foreign persons of interest as national security threats, with other U.S. government systems.[14] Further, DOD's Chief Information Officer directed

[14]On February 2, 2004, DOD's Chief Information Officer issued a memorandum, entitled "Department of Defense Compliance with Internationally Accepted Standard for Electronic Transmission and Storage of Fingerprint Data from 'Red Force' Personnel."

that all new and upgraded DOD biometric collection devices used to collect certain data[15] must conform to the FBI's mission-specific requirement and the devices must be certified as interoperable with the FBI's biometric systems.

In November 2005, the Army's Chief Information Officer reiterated the importance of standardization and interoperability of DOD's biometric systems in fighting terrorism and stated that conformance to standards strengthens DOD's abilities to fulfill its missions.[16] The memorandum further stated that all new or updated DOD collection devices must meet the DOD EBTS standard and be interoperable with DOD's biometric system ABIS. Consistent with the Army's position on interoperability, the DOD Directive on Biometrics, issued in February 2008, stated that collection and transmission of biometric information shall be controlled through the use of DOD adopted standards to enhance consistency and interoperability of biometric information.[17] A 2009 Joint Interoperability report, which reviewed selected biometric systems that interfaced with DOD's ABIS and analyzed data collected by these systems for conformance issues that have an impact on interoperability, stated that several DOD biometric collection devices meet DOD adopted standards.[18] For example, the Guardian, Fusion, and Secure Electronic Enrollment Kit for Identification all meet the EBTS standard current at the time of the report, specifically, EBTS version 1.2.

[15]The February 2004 memorandum directed that all new and upgraded DOD biometric collection devices used to collect "red force" fingerprint data must be certified as interoperable with the FBI's biometric systems. DOD officials told us that the HIIDE device may be used to collect such "red force" data.

[16]On November 29, 2005, the U.S. Army's Chief Information Officer issued a memorandum, entitled "Department of Defense Compliance with the Electronic Biometric Transmission Specification."

[17]DOD Directive 8521.01E, *Department of Defense Biometrics* § 4.3 (Feb. 21, 2008).

[18]Joint Interoperability Test Command, Baseline Interoperability Assessment Report of the Department of Defense Automated Biometric Identification System, version 1.0.13, (November 2009).

DOD Has Not Taken Certain Actions Needed to Help Ensure New and Updated Standards Are Implemented

DOD has not taken certain actions necessary to help ensure that its collection devices adhere to new and updated standards, including not having an effective process, procedure, or timeline for implementing updated standards, not routinely testing collection devices at sufficient levels of detail for conformance to these standards, and not fully defining roles and responsibilities to ensure accountability. For example, a collection device used by the Army to meet an urgent need in 2005 and currently still in use in Iraq and Afghanistan, did not meet the standard current at the time of the 2009 Joint Interoperability report, and according to DOD officials, continues to not adhere to DOD EBTS version 1.2 or the more current version 2.0. As of late 2009, this collection device, known as the Handheld Interagency Identity Detection Equipment or HIIDE, continued to be purchased by DOD. According to DOD officials, DOD continues to use the HIIDE because it meets DOD's mission needs and since it was developed as an urgent mission need for Central Command to collect and authenticate the identity of individuals, it does not have to adhere to DOD's information technology standards. Those standards are included in the DOD Information Technology Standards Registry, the central repository for DOD-approved information technology standards, and are mandated for programs of record for biometric technologies, which are considered permanent capabilities. Therefore urgent needs do not have to adhere to DOD adopted standards. According to information provided by BIMA about the composition of ABIS as of September 2010, the HIIDE device is responsible for the collection of 13 percent of the biometric records in ABIS, the largest number of submissions by a handheld device.

Because the HIIDE device does not conform to standards, DOD cannot seamlessly share biometric information from this device with other federal agencies. For example, of the approximately 4.8 million biometric records maintained by DOD, approximately 630,000 HIIDE biometric records cannot be searched automatically against the approximately 94 million biometric records in the FBI's system. Further, if the biometric information collected by the HIIDE is not stored in the FBI IAFIS system, DHS loses the benefit of searching its 119 million biometric records against HIIDE information as well. Both DOD and DHS access FBI's IAFIS in order to share information. Therefore, if FBI does not have access to DOD information, for example, HIIDE biometric records, then neither does DHS when they search against IAFIS. However, according to DHS and DOD officials, DOD manually provides biometric records of individuals on its watch list, which can include HIIDE-collected biometric information. These records are then manually added to DHS's IDENT. Without biometric collection devices that conform to DOD adopted

standards, DOD limits its and federal partners' ability to identify potential criminals or terrorists who have biometric records in other federal agency's biometric systems.

DOD Does Not Have an Effective Process, Procedure, or Timeline for Implementing Updated Standards

DOD would benefit from establishing or communicating a process, procedure, or timeline for implementing updated standards for biometric collection devices that are in the acquisition process. Although DOD has updated its EBTS standard several times, most recently from DOD EBTS version 1.2 to DOD EBTS version 2.0 in April 2010, it has not established or communicated to biometric stakeholders a process, procedure, or timeline for implementing the updated standard for biometric collection devices that are in the acquisition process. *The Standard for Program Management* states a program should adhere to technical standards, and should be managed as these technical standards are updated.[19] However, DOD did not provide the date that the most recently updated DOD EBTS standard would be mandated in a clear and timely way to ensure that military services responsible for acquiring biometric capabilities could plan to implement the updated standard on collection devices that were already in DOD's acquisition process.[20] For example, the Navy's acquisition of a collection device has been disrupted by late and conflicting information about when to conform to the new or updated standard. Prior to the adoption of DOD EBTS 2.0, the Navy, in November 2009, requested that BIMA provide information on which version of the EBTS standard to implement in its collection device that was already in the acquisition process. The Navy specifically requested in a letter that this information be provided by February 26, 2010, prior to major development milestones for the collection device, occurring in March 2010, to ensure that the device would meet the correct version of the standard. However, BIMA did not provide information to the Navy on the effective date of the updated standard or which version of the standard to implement in the device until a month after the device had reached the development milestones. In addition, DOD provided contradicting information to the Navy. On April 2, 2010, BIMA recommended the Navy use DOD EBTS version 1.2 for the standard for the collection device, but on the same day, the new DOD EBTS version 2.0 standard was adopted through the DOD

[19]The Project Management Institute, *The Standard for Program Management* © (2006). For the purposes of this report, we are referring to DOD's biometric program in its entirety, not the acquisition program for one particular biometric collection device.

[20]DOD standards are adopted through updates to the DOD Information Technology Standards Registry.

Information Technology Standards Registry, the central repository for DOD-approved information technology standards, as the biometric standard for use in all collection devices.

According to BIMA, additional guidance was not necessary for the current update to the DOD EBTS 2.0 standard because biometric stakeholders knew about the update since DOD EBTS version 2.0 was an emerging standard. BIMA also stated that emerging standards are provided to help military services plan for updates to DOD adopted standards, and an emerging standard should become a DOD adopted standard within 3 years. However, without timely guidance that documents and communicates a process, procedure, or timeline for updating biometric capabilities from one version of a standard to another, the military services may continue to lack accurate information that is necessary to implement new or updated standards during the acquisition process. Specifically, military services may not have information on when an emerging DOD standard will become mandated[21] within the 3-year time frame, but must ensure that collection devices being developed conform to the DOD mandated standard, not the emerging standard. The Army established the Biometrics Standards Working Group based on the 2008 biometric directive that, among other activities, it should provide guidance for consistent standards implementation, however, the 2009 DOD joint interoperability assessment found that DOD lacked a process beyond the Working Group to address the impact of changes to the DOD adopted standards. Further, absent such a process, procedure, or timeline to manage the update to new standards, the military services may also face increased costs in developing biometric collection devices when time frames for the update of standards are not documented or managed. Service officials said that the Navy's collection device would have to be updated to the new version of EBTS at the next major development milestone, incurring an additional cost for the

[21]Each standard accepted to the DOD Information Technology Standards Registry is assigned a status. One such status is referred to as "mandated standards." The DOD Information Technology Standards Registry defines "mandated standards" as "the minimum set of essential standards for implementation in the acquisition of all DOD systems that produce, use, or exchange information and, when implemented, facilitate the flow of information in support of the warfighter. These standards are mandated for the management, development, and acquisition of new or improving systems throughout the DOD." Department of Army, Biometrics Task Force, Biometrics Collection, Transmission and Storage Standards Technical Reference (July 24, 2006). In this report, the terms mandated and mandated DOD standards refer to the status assigned to such standards as defined in Biometrics Collection, Transmission and Storage Standards Technical Reference.

development of the collection device. Navy officials estimate that the service will incur $3.4 million in additional costs because of the delay.

DOD Does Not Routinely Test Devices at Sufficient Levels of Detail for Conformance to These Standards

DOD tests collection devices for conformance to adopted standards, but testing efforts have not always been at a sufficient level of detail or integrated to facilitate interoperability across DOD and federal agencies.[22] The National Science & Technology Council's policy for enabling the development, adoption, and use of biometric standards acknowledges that the capability to share biometric information will be dependent on rigorous conformance testing.[23] BIMA conducts standards conformance testing to evaluate conformance of collection devices to DOD adopted standards, but the 2009 joint interoperability assessment found that conformance testing efforts have not been integrated and formalized into the biometric enterprise's processes and procedures that are necessary to facilitate interoperability across DOD and with interagency partners. In addition, a BIMA official told us that the conformance testing done at BIMA is not sufficiently detailed to ensure that collection devices conform to DOD adopted standards. Since certain DOD collection devices were acquired to meet urgent needs, DOD may have relied on vendors to provide devices that purport to, but may not, conform to DOD adopted standards. Without an integrated and formalized process for sufficiently detailed conformance testing, DOD has no mechanism to hold vendors accountable for ensuring that biometric collection devices meet DOD adopted standards.

DOD issued a biometrics program directive in February 2008, and a companion draft instruction could provide some guidelines, including on the testing of biometric collection devices for conformance to standards and interoperability.[24] Based on our review of the draft instruction though, it is unclear that it will provide guidance on a process that holds DOD biometric stakeholders accountable for collection devices that conform to standards. Without a process that ensures collection devices are tested at

[22]Chairman of the Joint Chiefs of Staff, Instruction (CJCSI) 6212.01E requires results from standards conformance testing to be part of the interoperability evaluation. The Joint Interoperability Test Command has conducted interoperability evaluations on its biometrics systems, though it was a limited assessment due to a lack of conformance testing by DOD.

[23]National Science & Technology Council, Subcommittee on Biometrics and Identity Management, NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards (Sept. 7, 2007).

[24]DOD Directive 8521.01E, *Department of Defense Biometrics* (Feb. 21, 2008).

a sufficiently detailed level to conform to DOD adopted standards and that holds DOD biometric stakeholders accountable for device conformance, DOD limits its ability to collect biometric information that is interoperable with other federal agency systems.

DOD Has Not Fully Defined Roles and Responsibilities Specifying Accountability Needed to Ensure Its Collection Devices Meet New and Updated Standards

DOD has a biometric program directive, but could more fully define the roles and responsibilities of DOD entities with the intention of instilling accountability for ensuring its collection devices meet new or updated standards. The Office of Management and Budget guidance on establishing internal controls emphasizes that agencies should ensure accountability for results, and our work on internal controls states that defined roles and responsibilities are needed to achieve an organization's mission.[25]

DOD's February 2008 biometric program directive assigned some roles and responsibilities to DOD biometric stakeholders, such as designating the Office of the Director for Defense, Research and Engineering, as the Principal Staff Assistant responsible for oversight of DOD biometrics programs and policies.[26] However, based on our review of the directive and according to agency officials, DOD has not fully clarified the differing responsibilities that each DOD biometric stakeholder has in ensuring that collection devices conform to adopted standards. In addition, according to DOD officials, DOD has not clarified roles and responsibilities for DOD biometrics and this has caused confusion related to overlapping responsibilities and accountability within Army entities, such as whether BIMA can send requirements for acquiring biometrics capabilities directly to the program manager or whether such requirements should be provided by Army officers and staff responsible for operational requirements. The Office of Management and Budget's guidance on establishing internal controls emphasizes that agencies should design management structures for programs to help ensure accountability for results.[27] Moreover, GAO's *Standards for Internal Control in Federal Government* states that management structures should establish and document roles and

[25]OMB Circular No. A-123, *Management's Responsibility for Internal Control* (Washington, D.C., December 2004), and GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999). OMB issued Circular A-123, revised December 21, 2004, to provide the specific requirements for assessing the reporting on internal controls. Internal control standards and the definition of internal control in Circular A-123 are based on GAO's *Standards for Internal Control in the Federal Government*.

[26]DOD Directive 8521.01E, *Department of Defense Biometrics* § 1.2 (Feb. 21, 2008).

[27]OMB Circular No. A-123.

responsibilities needed to achieve an organization's mission and objectives, and that such documentation should be approved, current, and binding on all appropriate stakeholders.[28]

DOD recognized that further guidance may be needed to implement the biometrics directive and began developing a draft instruction that would clarify the roles and responsibilities of DOD biometric stakeholders. However, the instruction has been in draft since 2008, and continues to be in draft as of February 2011. A DOD official told us that the instruction is being updated to include a larger oversight role for the Office of the Director for Defense, Research and Engineering, especially for oversight of the Army's role as DOD's biometrics Executive Agent. It is not clear that DOD's draft instruction, when completed, will improve stakeholders' understanding of roles and responsibilities for DOD biometric activities. For example, with the March 2010 DOD change of the Biometrics Task Force to BIMA it is unclear if the new instruction would include redefined roles and responsibilities associated with BIMA. DOD officials told us that the only documentation they received about the change of the Biometrics Task Force to BIMA was a memorandum in March 2010 that simply stated the name change, but contained no additional information on roles and responsibilities. Further, DOD documents that could provide some clarity to roles and responsibilities by assigning specific actions to DOD biometric stakeholders have not been updated to reflect the change, such as the *Biometric Enterprise Strategic Plan 2008-2015* and the corresponding *Implementation Plan*. According to BIMA officials, both the *Biometric Enterprise Strategic Plan* and its corresponding *Implementation Plan* are currently being revised. DOD has an opportunity to further clarify roles and responsibilities through its implementing instruction to help ensure that collection devices are interoperable with other federal agencies.

[28] GAO/AIMD-00-21.3.1.

DOD Is Sharing Biometric Information but Sharing Is Limited by the Absence of an Agreement with DHS and DOD's System Capacity

DOD is sharing its biometric information and has an agreement to share biometric information with DOJ, which allows for direct connectivity and the automated sharing of biometric information between their biometric systems. However, DOD's ability to optimize sharing is limited by not having a finalized sharing agreement with DHS,[29] and its capacity to process biometric information. Currently, DOD and DHS do not have a finalized agreement in place to allow direct connectivity between their biometric systems, due to the need for additional reviews of the proposed agreement by certain DHS officials, among others. DOD is working with DHS to develop a memorandum of understanding to share biometric information now scheduled for completion in May 2011; however, without the agreement, it is unclear whether direct connectivity will be established between DOD and DHS, which affects response times to search queries. In addition, agencies' biometric systems have varying system capacities based on their mission needs, which affects their ability to similarly process each other's queries for biometric information. Moreover, the advancements other agencies make in their biometric systems may continue to overwhelm DOD's efforts as it works to identify its long-term biometric system capability needs and associated costs.

DOD Has an Agreement with DOJ, Which Allows for Direct Connectivity and Automated Sharing of Biometric Information

DOD is sharing its biometric information and has an agreement to share biometric information with DOJ, which allows for direct connectivity and the automated sharing of biometric information between their biometric systems. DOD and the FBI (a component of DOJ) have an agreement in place that allows for direct connectivity and the automated sharing of unclassified biometric information between their biometric systems. Until DOD and DHS establish direct connectivity between their two biometric systems, they have the option to use the FBI's biometric system as an indirect link to share limited biometric information (see fig. 3 below).[30] Additionally, as mentioned earlier, according to DOD and DHS officials, DOD manually provides DHS with biometric records on watch listed individuals. In support of national directives and laws directing federal agencies to share information, the DOD directive on biometrics directs the

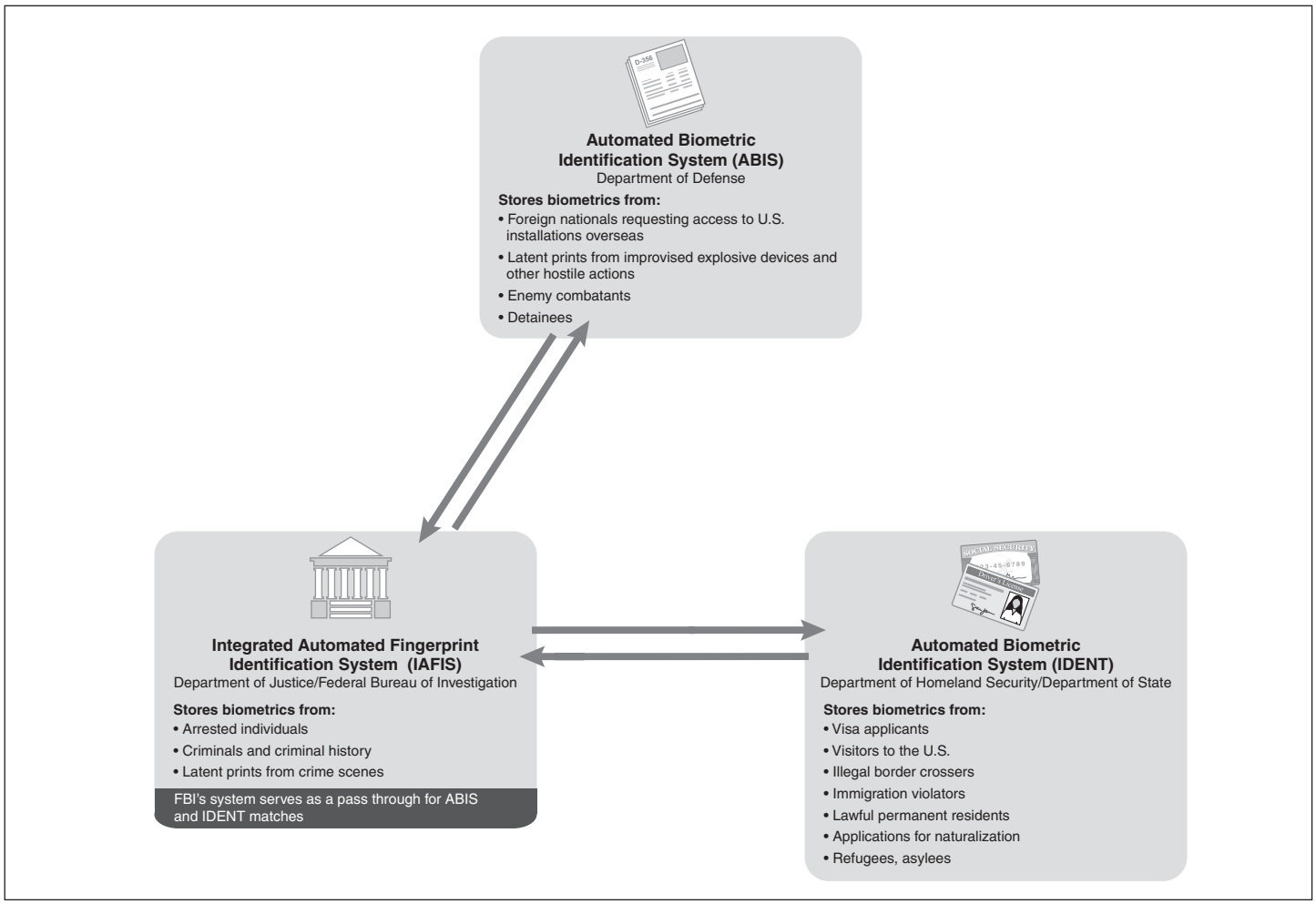
[29]DOD does not have an agreement in place to directly share information with State, and there are no plans to establish direct connectivity between DOD and State. State utilizes DHS's biometric system for sharing State's biometric information with other key federal agencies.

[30]Memorandum of Understanding Between the Federal Bureau of Investigation and the Department of Defense for Sharing of Biometric and Other Identity Management Information, September 2009. The FBI is a component of DOJ.

development of interagency agreements for biometrics activities, as appropriate, to maximize effectiveness. According to officials from the Office of the Under Secretary of Defense for Policy,[31] in 2003 the FBI formally requested that DOD share biometric information, and from that point, the agencies established data sharing with each other. DOD and the FBI finalized the memorandum of understanding in 2009 to provide for the sharing of, among other things, unclassified biometric information, as part of the agencies' efforts to comply with the National Security Presidential Directive-59/Homeland Security Presidential Directive-24. As part of the memorandum, DOD and the FBI agree to share their biometric information with each other in a timely manner when their respective missions require access to such data.

[31]DOD Directive 8521.01E, *Department of Defense Biometrics* § 5.2.2 (Feb. 21, 2008), designates responsibility to the Under Secretary of Defense for Policy to prepare and issue interagency agreements, among other things, for biometrics activities, as appropriate.

Figure 3: Current Biometric Information-Sharing Connectivity between DOD, DOJ/FBI, and DHS/State



Source: GAO analysis of information provided by DOD.

In addition to DOD and the FBI's agreement to share biometric information, DHS, State, and DOJ have agreements in place that allow for direct connectivity and the automated sharing of biometric information among their biometric systems—capabilities that support the collection, storage, use, and sharing of biometric data. Specifically, DHS and State established a memorandum of understanding in 2005 to facilitate interagency cooperation and sharing of, among other things, biometric information on visa applicants and biometric information stored on DHS's biometric system, to enhance border security and facilitate legitimate

travel.[32] State uses DHS's biometric system for storing and sharing copies of their biometric information.[33] Additionally, DHS, DOJ, and State established a memorandum of understanding in July 2008 to improve information sharing among the three agencies for the purposes of such missions as national security, law enforcement, immigration, and border management.[34] The July 2008 memorandum included an agreement to share, among other things, biometric information through interoperability between the agencies' biometric systems. According to FBI officials, the FBI initiated the interoperability agreement in 2005 to exchange biometric information between DOJ's and DHS's biometric systems and gained access to DHS's full biometric system in 2008. However, according to DHS officials, initial sharing of DHS high priority biometric information with DOJ's biometric system began in 2006, such as information on individuals expedited for removal and those denied visas.

DOD Does Not Have an Agreement with DHS or with State, Which Limits Its Ability to Efficiently Share Biometric Information

DOD and DHS currently do not have an agreement in place that allows for direct connectivity between their biometric systems; however, DOD is currently in the process of working with DHS to develop a memorandum of agreement to share biometric information. DOD also does not have an agreement in place to directly share information with State; however, according to DOD officials, State sharing requirements will be covered in the agreement between DOD and DHS.[35] According to the draft memorandum, the intent of the document is to formalize the ongoing relationship between DOD and DHS and to clarify their commitment to permitting the maximum amount of biometric information sharing permitted by law. Among other delays, in July 2010, DOD officials informed us that the draft memorandum was undergoing a subsequent review at DHS because some individuals at DHS had been inadvertently

[32]Memorandum of Understanding Between the Department of State and the Department of Homeland Security for Cooperation in: Enhanced Border Security – the US-VISIT Program, the Biometric Visa Program, and the Visa Datashare Program, January 2005.

[33]There are no plans to establish direct connectivity between State and DOJ, according to State officials.

[34]Memorandum of Understanding Among the Department of Homeland Security, the Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division; and the Department of State, Bureau of Consular Affairs for Improved Information Sharing Services, July 1, 2008.

[35]There are no plans to establish direct connectivity between DOD and State, according to State officials.

left off the initial review. As of January 2011, DOD and DHS have not signed an agreement that allows for direct connectivity between their biometric systems.

We reported in 2008 that DHS officials acknowledged that establishing a sharing agreement with DOD would increase sharing of biometric information between the agencies and close any gaps.[36] According to DHS officials, having such an agreement in place would allow DOD and DHS to access each other's biometric systems when needed for reasons such as detainee screening and airport passenger screening. Direct access would reduce response times to search queries because currently DOD and DHS biometric systems do not have direct connectivity and therefore do not have automated search capabilities so the response times vary. We recognize that developing an agreement to share information takes time; for example, it took over 5 years to develop the memorandum of understanding between DOD and the FBI. DOD and DHS officials stated they had hoped to have the memorandum completed by the end of 2010; however, as of January 2011 the agreement had not yet been completed. Several dates of completion and reasons for delay of the memorandum between DOD and DHS were provided to us by DOD officials throughout our review. In December 2010, DOD anticipated completing a signed agreement with DHS no later than May 31, 2011.

According to DOD and DHS officials, some sharing of information is occurring between DOD, DHS, and State, even though DOD and DHS do not have a finalized sharing agreement. We reported in 2008 that DOD and DHS had not established direct connectivity between their two biometric systems and relied on the FBI's biometric system as an indirect link between DOD and DHS. At the time, while limited occasional sharing of DOD and DHS biometrics occurred, it did not happen on a regular basis. According to DOD, DHS, and FBI officials, the indirect sharing arrangement through the FBI's biometric system is still in place, as shown in figure 3. The FBI maintains an Interim Data Sharing Model, which consists of two parts—the FBI provides a set of data to DHS for DHS stakeholders to access and DHS provides a set of data to the FBI for FBI stakeholders to access, to include DOD, which includes biometric information on individuals with expedited removals and individuals who

[36]GAO, *Defense Management: DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing*, GAO-09-49 (Washington, D.C.: Oct. 15, 2008).

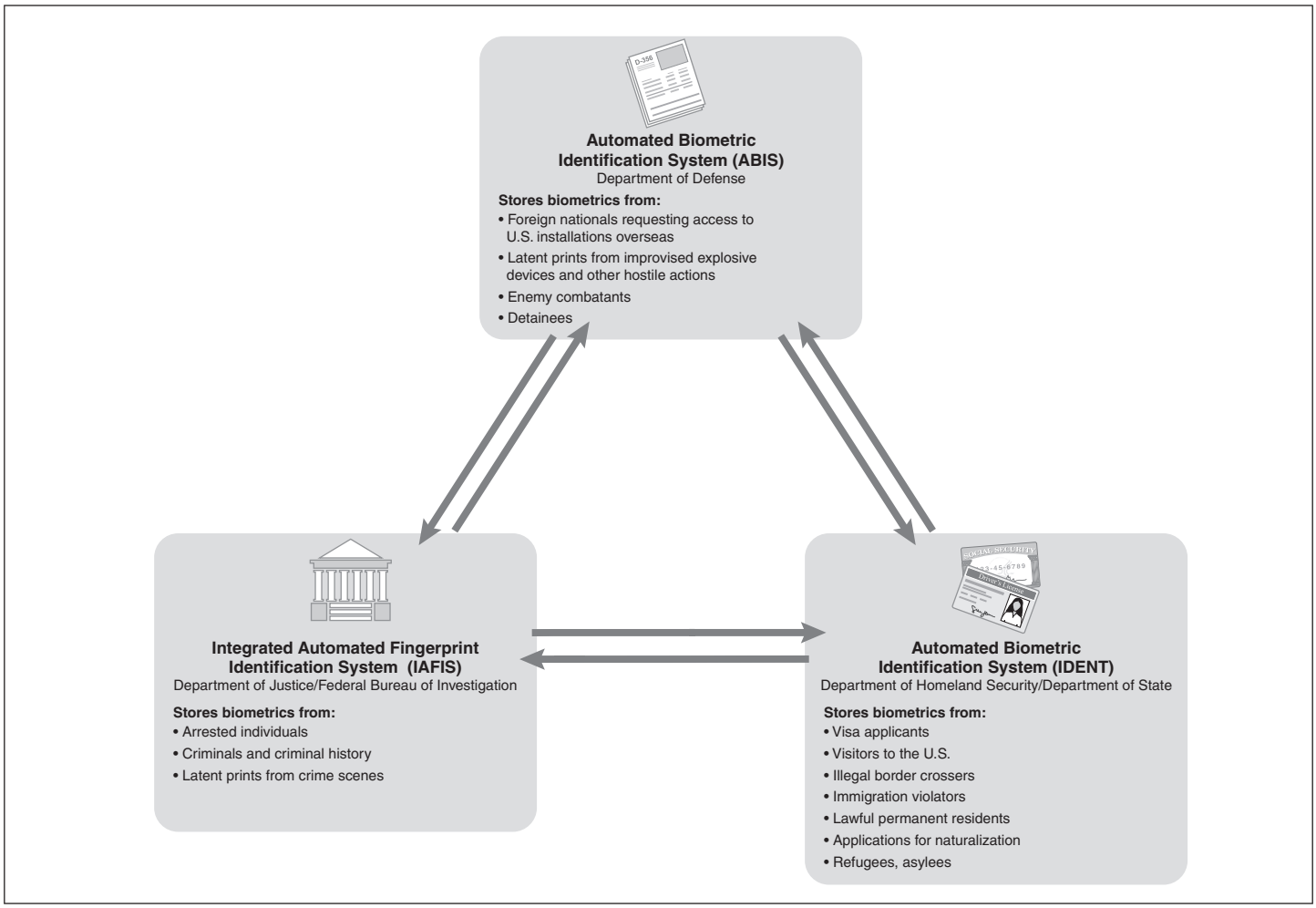
were denied visas. Furthermore, the FBI retains on its IAFIS some biometric information from DOD on non-U.S. persons, such as those who have criminal records, which allows DHS and State to access limited information from DOD through the FBI biometric system. However, both DOD and FBI officials noted that the FBI may be terminating its Interim Data Sharing Model as the FBI transitions to its new biometric system. In March 2011, FBI officials reported that DOD searches of the portion of the Interim Data Sharing Model containing information on expedited removals and individuals who were denied visas were discontinued on January 20, 2011. However, FBI's IAFIS will continue to facilitate searches of DHS information for DOD until a direct connection has been established between DHS and DOD's biometric systems, according to FBI officials.

Since we reported in 2008, DOD and DHS have established a manual process for sharing information on at least a daily basis—once every 24 hours—through the use of a secured Web site. DOD manually inputs to this web site copies of critical DOD biometric information that DHS can manually access to place onto its own biometric system. The State Department can access this information once it is stored on DHS's biometric system. However, DHS and State may not be able to take immediate action should they have a query prior to DOD's once-a-day update. In addition, as noted in our 2008 report,[37] if DHS and State do not have access to DOD biometric information on individuals trying to enter the United States, then they may not be able to determine whether those individuals should be denied entry, and potential harm could come to U.S. interests from individuals inadvertently allowed into the United States.

Officials from DOD, DHS, and the FBI have discussed the goal for direct connectivity among their biometric systems to better enable automated sharing of biometric information (see fig. 4). However, as noted earlier, without a finalized agreement between DOD and DHS, it remains unclear when or whether direct connectivity will be established between DOD's and DHS's biometric systems.

[37] GAO-09-49.

Figure 4: Desired Biometric Information-Sharing Connectivity between DOD, DOJ/FBI, and DHS/State



Source: GAO analysis of information provided by DOD.

DOD's Biometric System Is Limited in Meeting Demands from Key Federal Agencies' Biometric Systems

To enable agencies to meet the demand for searching stored biometric information on their systems, agencies' biometric systems have varying system capacities based on their mission needs, which affects their ability to similarly process each other's queries for biometric information. As noted previously, the FBI's IAFIS is a national fingerprint and criminal history system, while DHS's IDENT is used for many purposes, including border security and visa and naturalization processing. DOD's Next Generation ABIS is used to identify and verify non-U.S. persons and helps

determine if the individual poses a threat or potential threat to national security. DOD's Next Generation ABIS is currently capable of handling 8,000 transactions per day. In contrast, according to FBI officials, the FBI's IAFIS system currently performs over 100,000 to 200,000 search queries a day, while DHS manages over 160,000 search queries a day, according to DHS officials. DOD has plans to increase the capacity to 22,000 transactions per day in the third quarter of fiscal year 2011 and upgrades to later bring capacity up to 45,000 transactions per day, according to DOD officials.

DOD officials do not believe that they need to match other agencies' biometric system capacities because they do not anticipate receiving the same number of queries given differences in mission. However, DOD and other agency officials have expressed concern that DOD's biometric system is limited in its ability to maximize sharing of biometric information. The FBI has reported that DOD is currently meeting their needs by supporting a capacity of 3,000–4,000 transactions per day, for which the FBI could query DOD's Next Generation ABIS to search against. However, FBI officials told us that they are concerned with DOD's capacity as the Next Generation ABIS is not capable of handling all of the queries that the FBI receives. FBI officials noted that DOD does not want the FBI to send every search query it receives through DOD's biometric system. At this time, the FBI and DOD are working to target and define a set of search queries for the FBI to send through Next Generation ABIS, according to FBI officials. However, a maximum transaction capacity has not yet been set for FBI submissions to DOD. Additionally, DHS officials believe DOD will need more capacity to handle search queries in order for direct interoperability between DOD and DHS to occur. DHS reported in November 2010 that when it establishes direct interconnectivity with DOD, DHS plans to send 13,000 search queries in 2011 and 14,000 search queries in 2012 to DOD's Next Generation ABIS for searching per day. DHS noted in January 2011 that transaction volumes for search queries from DHS to DOD's biometric system are currently in flux and have not been finalized. However, DOD officials have acknowledged that their current system's transaction capacity is limited for sharing because the number of queries from other federal agencies currently exceeds their biometric system capacity of 8,000 transactions per day.

The advancements other agencies continue to make in their biometric systems may overwhelm DOD's efforts as it works to identify its long-term biometric system capability needs and associated costs. At the same time that DOD carries out these expansion efforts, other agencies continue to make advancements in their biometric systems and will continue to do so

in the future for various reasons, including the addition of new technology and biometric modalities as emerging technologies and modalities are identified and matured. For example, as previously mentioned, DHS is considering iris and facial biometrics for future incorporation into its biometric system. In addition, the FBI is moving to an enhanced biometric system that will incorporate scars, marks, tattoos, face, iris, and palm biometrics. Such agency biometric system advancements could exceed DOD's biometric system's capability to respond. In light of this, DOD may not be able to facilitate sharing of biometric information across federal agencies in a timely and efficient manner, in accordance with DOD policies. Specifically, DOD's biometric directive requires that biometric systems be interoperable with other identity management capabilities and systems both internal and external to DOD, to maximize effectiveness, as well as information-sharing efforts.[38] Furthermore, DOD's biometrics strategic plan outlines as a primary objective that DOD operate and maintain biometric systems that enable sharing with other biometric systems as part of DOD's goal to meet the warfighters' needs in a timely manner.[39]

Conclusions

National security challenges from multiple sources continue to increase, therefore making it critical that federal agencies find effective ways to collaborate and share information—particularly biometric information—on those who would threaten the United States. DOD has taken steps to adopt biometric standards that could improve the quality of biometric information collected and has increased its efforts to share biometric information with key federal agencies. However, DOD could take certain actions to help improve its ability to collect and share biometric information with other federal agencies. For example, DOD has adopted standards for the collection of biometrics to enhance interoperability with other key federal agencies' biometric systems, but at least one DOD device responsible for the collection of over 600,000 biometric records, does not meet DOD adopted standards, such as a handheld biometric collection

[38]DOD, Directive 8521.01E, *Department of Defense Biometrics* § 4.4 and § 4.11 (Feb. 21, 2008). The Intelligence Reform and Terrorism Prevention Act created an Information Sharing Environment, defined as an approach that facilitates the sharing of terrorism and homeland security information, with a Program Manager responsible for information sharing across the federal government. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, § 1016 (2004).

[39]Department of Defense *Biometrics Enterprise Strategic Plan, 2008 – 2015* (Aug. 27, 2008).

device used by the Army. DOD can take steps to improve conformance to DOD adopted standards with a process for implementing updated standards for biometric collection devices that are in the acquisition process, more sufficient testing of devices for conformance to adopted standards to better facilitate interoperability with federal agencies, and more fully defining the roles and responsibilities of DOD entities to ensure its collection devices meet DOD adopted standards. Without these steps, DOD limits its ability to identify potential criminals or terrorists who have biometric records in other federal agency's biometric systems, and may result in the military services incurring delays and additional costs if they find they have acquired a device that is no longer acceptable to DOD. In addition, DOD has agreements in place with key federal agencies such as DOJ to help facilitate direct connectivity between their biometric systems, but it has not finalized an agreement with DHS and by extension the State Department. This has an impact on timely interoperability. Finally, the varying system capacities at these key federal agencies exceeds that of DOD to the extent that agencies have expressed concern that DOD's biometric system may be unable to meet the search demands from their own biometric systems within useful response time frames. Without efforts to address these issues, the quality and process of collecting and sharing biometrics may continue to limit DOD's ability to identify potential criminals or terrorists who have biometric records in other federal agency's biometric systems in a timely manner, and ultimately these challenges to interoperability may place U.S. national security at greater risk.

Recommendations for Executive Action

To improve DOD's ability to collect and help ensure that federal agencies are sharing biometric information on individuals who pose a threat to national security to the fullest extent possible, we recommend that the Secretary of Defense direct the Under Secretary of Defense for Acquisition, Technology, and Logistics, as the Principal Staff Assistant responsible for the oversight of DOD biometrics, to take the following five actions in collaboration with other key federal agencies and internal DOD stakeholders, including BIMA, U.S. Army, U.S. Navy, U.S. Marines, and U.S. Air Force:

- Implement a process for updating collection devices to adopted standards to help ensure that all DOD systems related to biometrics, including collection devices, conform to adopted standards.
- Implement a process for testing collection devices at a sufficiently detailed level to help ensure that all DOD systems related to biometrics, including collection devices, conform to adopted standards.

- More fully define and further clarify the roles and responsibilities needed to achieve DOD's biometric program and objectives for all stakeholders that include ensuring collection devices conform to adopted standards.
- Complete the memorandum of agreement with the Department of Homeland Security regarding the sharing of biometric information as appropriate and consistent with U.S. laws and regulations and international agreements, as well as information-sharing environment efforts.
- Identify its long-term biometric system capability needs, including the technological capacity and associated costs needed to support both the warfighter and to facilitate sharing of biometric information across federal agencies, and take steps to meet those capability needs, as appropriate and consistent with U.S. laws and regulations, international agreements, and available resources.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD agreed with all of our recommendations. DOD's comments appear in their entirety in appendix III. DHS DOJ, State, and the Department of Commerce/National Institute of Standards and Technology also reviewed a draft of this report. We received technical comments from DHS and DOJ, which we have incorporated as appropriate.

DOD agreed with our recommendation to implement a process for updating collection devices to adopted standards to help ensure that all DOD systems related to biometrics, including collection devices, conform to adopted standards. In its response, DOD noted that the legacy HIIDE devices are near the end of their service life and are being retired. DOD intends to procure an updated handheld device compliant with the mandated data standard to replace the HIIDE, which was EBTS 1.2 at the time the solicitation was developed and published, and as required by DOD Directive 8521.01E for all new acquisitions. DOD expects to award this contract in April 2011, with fielding in August 2011. DOD further stated that DOD's Biometrics Standards Conformity Assessment Test Program plans to verify compliance of the updated handheld devices before deployment, and DOD plans additional engineering efforts to update devices to the recently adopted EBTS 2.0 standard to ensure compatibility with interagency partners.

DOD agreed with our recommendation to implement a process for testing collection devices at a sufficiently detailed level to help ensure that all DOD systems related to biometrics, including collection devices, conform to adopted standards. In its response, DOD stated that it has established a Biometrics Standards Conformity Assessment Test Program, accredited in

January 2011 as part of the National Institute of Standards and Technology's (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) for biometric testing. Relevant tests include conformance tests to DOD EBTS and FBI Electronic Fingerprint Transmission Specification, as well as evaluations and assessments of biometric-enabled devices and systems that interoperate with the authoritative biometrics database and other repositories of biometric data. DOD added that the current DODD 8521.01E already requires such compliance testing for new biometrics acquisitions, but DOD noted and we agree that the directive does not fully address quick reaction capabilities such as the HIIDE. DOD further added that it plans to work with the FBI to develop a co-sharing arrangement to leverage existing standards compliance testing at the FBI Biometric Center of Excellence to strengthen interagency interoperability. DOD stated that it plans to include these requirements in the biometric DOD directive no later than September 2011. We agree that incorporating into the biometric DOD directive the requirements of conformance testing of biometric systems through the newly established Biometrics Standards Conformity Assessment Test Program, conformance testing for all biometric devices, and co-sharing arrangements with FBI Biometric Center of Excellence would be beneficial.

DOD agreed with our recommendation to more fully define and further clarify the roles and responsibilities needed to achieve DOD's biometric program and objectives for all stakeholders that include ensuring collection devices conform to adopted standards. In its response, DOD indicated that it is updating DOD Directive 8521.01E "Defense Biometrics," which establishes policy, assigns responsibilities, and describes procedures for DOD biometrics. DOD further noted that the update to the DOD biometrics directive will more fully define and clarify the roles and responsibilities of biometrics stakeholders, including responsibilities for testing collection devices for compliance with adopted standards. According to DOD, the biometric directive will be completed by September 2011.

DOD agreed with our recommendation to complete the memorandum of agreement with the Department of Homeland Security regarding the sharing of biometric information as appropriate and consistent with U.S. laws and regulations and international agreements, as well as information-sharing environment efforts. On February 14, 2011, we provided DOD a draft of this report for review and comment. In response to our draft recommendation, and while the report was under review, DOD finalized an agreement with DHS regarding biometric sharing on March 3, 2011.

DOD agreed with our recommendation to identify its long-term biometric system capability needs, including the technological capacity and associated costs needed to support both the warfighter and to facilitate sharing of biometric information across federal agencies, and take steps to meet those capability needs, as appropriate and consistent with U.S. laws and regulations, international agreements, and available resources. In its response, DOD noted that ABIS is currently meeting all the sharing transactions required by DHS and FBI, and DOD has expansion plans in place to increase ABIS's capability to over 40,000 daily transactions, which according to DOD will continue to meet the 14,000 daily biometrics transaction rate articulated by DHS for 2012. Further, DOD stated that it continues to work closely with the interagency Interoperability Executive Steering Committee to ensure DOD has visibility as new interagency requirements coalesce, and can modify ABIS expansion plans to be responsive to our interagency sharing responsibilities. According to DOD, it expects to have an updated ABIS sizing plan to support the projected future DOD and interagency transaction requirements by July 2011.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees; the Secretary of Defense; the Secretary of State; the Attorney General; Secretary of Commerce; the Secretary of Homeland Security, and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff has any questions about this report, please contact me at (202) 512-5431 or at dagostinod@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be founds on the last page of this report. Key contributors to this report are listed in appendix IV.

Davi M. D'Agostino
Director
Defense Capabilities and Management

List of Requesters

The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable W. "Mac" Thornberry
Chairman
Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
House of Representatives

The Honorable Jim Langevin
Ranking Member
Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
House of Representatives

The Honorable Jeff Miller
House of Representatives

Appendix I: Scope and Methodology

This report addresses the extent to which DOD (1) adopted standards and has taken actions to facilitate the collection of biometrics that are interoperable with other key federal agencies, and (2) shares biometric information across key federal agencies.

Scope and Methodology

To address our objectives, we reviewed prior GAO reports related to the collection, storage, use, sharing, and management of biometric information and interagency sharing of information for national security purposes. We also analyzed a number of Presidential Directives, Executive Orders and Memorandums, and laws that affect the collection and sharing of biometric and biographic information. For example, we analyzed the National Security Presidential Directive-59/Homeland Security Presidential Directive-24 and the companion action plan for Biometrics for Identification and Screening to Enhance National Security, which establish a framework to ensure that federal executive departments and agencies use compatible methods and procedures for the collection and sharing of identity information across federal departments and agencies. In addition, we reviewed national strategies focused on information sharing and national security to gain an understanding of how biometrics collection and sharing plays a part in achieving national goals of gathering and sharing information to protect the United States.

We contacted and obtained information from officials and entities associated with the collection, storage, use, and sharing of biometric information across the Department of Defense (DOD), as well as other key federal agencies,[1] including the Department of Justice (DOJ)/Federal Bureau of Investigation (FBI), Department of State (State), and the Department of Homeland Security (DHS). Further, we conducted an interview with officials of the National Science and Technology Council to determine the role and interests that the White House has in biometrics.[2]

[1]We identified DOD, DHS, DOJ/FBI, and State as key federal agencies in the collection and sharing of biometric information. DOD, DOJ, and DHS have responsibility for our nation's security and maintain three major federal biometric systems that are used to prevent harm to our nation's security, and State helps protect our national security through the use of vital information from these systems to screen potential foreign visitors who may want to harm our nation.

[2]The National Science and Technology Council is responsible for the Committee on Technology, which has a Subcommittee on Biometrics and Identity Management. The National Science and Technology Council falls under the purview of the Office of Science and Technology Policy in the Executive Office of the President.

We conducted site visits to a selection of facilities that analyze, store, and share biometric information, including the Army's National Ground Intelligence Center, in Charlottesville, Virginia; the Army's Biometric Identity Management Agency; and the FBI's Criminal Justice Information Services complex, both located in Clarksburg, West Virginia; to discuss the use of applicable standards, federal agency biometric systems interoperability, and to gain perspective on the sharing of biometric information between federal agencies. We met with U.S. Central Command and U.S. Special Operations Command officials to obtain their views on how these two combatant commands had operationalized the collection of biometric information. More detailed information on the federal agencies and officials we obtained information from on the collection, use, storage, and sharing of biometric information during our review appears below in table 1.

Table 1: Agencies Where GAO Obtained Documentary Evidence and Officials' Views on the Collection, Use, Storage, and Sharing of Biometric Information

Federal agency	Entities visited or contacted during our review
Executive Office of the President	• Office of Science and Technology Policy, National Science and Technology Council, Committee on Technology, Subcommittee on Biometrics and Identity Management
Department of Commerce	• National Institute of Standards and Technology
Department of Defense	• Under Secretary of Defense for Acquisitions, Technology, and Logistics; Director, Defense Research and Engineering • Assistant Secretary of Defense for Networks and Information Integration • Under Secretary of Defense for Policy • Department of the Army, Biometric Identity Management Agency • Department of the Army, National Ground Intelligence Center • Headquarters, Department of the Army, G-3/5/7, Capability Integration Division • Department of the Army, Program Executive Office, Enterprise Information Systems, Program Manager, Biometrics • Department of the Air Force, Office of the Secretary of the Air Force, Communications Directorate • United States Marine Corps, Plans, Policies & Operations • Department of the Navy, Deputy Assistant Secretary of the Navy, Expeditionary Warfare • U.S. Africa Command • U.S. Central Command • U.S. European Command • U.S. Northern Command • U.S. Pacific Command • U.S. Special Operations Command • U.S. Southern Command

Federal agency	Entities visited or contacted during our review
Department of Homeland Security	• United States Visitor and Immigrant Status Indicator Technology Office • Immigration and Customs Enforcement • Customs and Border Protection • Screening and Coordination Office • U.S. Coast Guard
Department of Justice	• Federal Bureau of Investigation, Criminal Justice Information Services • Office of the Deputy Attorney General
Department of State	• Consular Affairs

Source: GAO.

To determine the extent to which DOD adopted standards and has taken actions to facilitate the collection of biometrics that are interoperable with other key federal agencies, we interviewed DOD officials and reviewed key DOD memoranda, directives, and guidance, such as the DOD Directive on Biometrics. In addition, we interviewed officials from DHS, State, and DOJ/FBI to gain their perspective on the collection and sharing of comparable biometric information among federal agencies. We reviewed national standards and requirements for the electronic formatting of biometric information to see whether key federal agencies follow a common set of standards for the collection of biometric information. For example, we reviewed DOD's Electronic Biometric Transmission Specification, which is based on recommended standards from the American National Standards Institute and the National Institute of Standards and Technology. We interviewed officials from the National Institute for Standards and Technology in order to obtain their perspective on the use of standards for the consistent collection of biometric information and how these standards are adopted by federal agencies to help ensure interoperability of the devices used to collect biometric information. We reviewed a DOD interoperability assessment report of its Automated Biometric Identification System and Army evaluations of the Handheld Interagency Identity Detection Equipment to identify DOD's interoperability and conformance to standards within these systems. We did not evaluate the technical performance of collection devices used to gather identity information. We discussed with federal agency officials the potential impact of collection devices and systems that do not conform to adopted standards on their ability to collect comparable biometric information. In addition, we reviewed key DOD biometric documentation to determine DOD management practices related to the collection of biometrics and interviewed key officials from DOD responsible for the management of the collection of biometrics. (See above table 1). Specifically, using criteria on internal control and program management

from the Office of Management and Budget and the Project Management Institute's The Standard for Program Management, we analyzed DOD guidance on the collection of biometrics to determine whether any internal control or program management weakness may reduce its ability to collect biometric information and meet biometric mission objectives. To gather the perspective of DOD biometric program management, we interviewed DOD biometric stakeholders such as the military services, Biometric Identity Management Agency, and combatant commands. In addition, we interviewed agency officials from the FBI and DHS to gather their perspectives on DOD's management practices related to the collection of biometrics.

To determine the extent to which biometric information is shared and has the system capacity needed to facilitate biometric sharing across key federal agencies, including DOD, we interviewed officials from DOD, DHS, State, and the FBI on the policies, governance processes, and systems in place for sharing biometric information—DOD's Automated Biometric Identification System (ABIS), DHS's Automated Biometric Identification System (IDENT), and the FBI's Integrated Automated Fingerprint Identification System (IAFIS). We analyzed the formal and draft agreements for sharing biometric information between agencies to better understand the scope of the biometric information shared, as well as any limitations, and the degree to which they help facilitate direct connectivity between the biometric systems to promote automated sharing.[3] In addition, we collected and reviewed federal policies, guidance, and other documentation that covered the sharing of biometric information and the current and planned systems that support biometric information sharing. For example, we reviewed DHS's IDENT Data Response Sharing Policy, which reinforces the DHS agreement with State and DOJ/FBI on sharing biometric information. We reviewed information provided by the FBI on IAFIS and their planned changes to the Next Generation Identification system that would expand their biometric capabilities from fingerprints to include the collection, matching, storage, and sharing of other biometrics

[3]Memorandum of Understanding Between the Department of State and the Department of Homeland Security for Cooperation in: Enhanced Border Security – the US-VISIT Program, the Biometric Visa Program, and the Visa Datashare Program, January 2005; Memorandum of Understanding Among the Department of Homeland Security; the Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division; and the Department of State, Bureau of Consular Affairs for Improved Information Sharing Services (July 1, 2008); and Memorandum of Understanding Between the Federal Bureau of Investigation and the Department of Defense for Sharing of Biometric and Other Identity Management Information (Sept. 2009).

such as facial and iris images. In order to confirm information provided by agency officials in interviews on the three primary biometric systems, we developed a structured questionnaire that was pre-tested and provided to key agency officials responsible for each of the three biometric systems.

We conducted this performance audit from December 2009 through March 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Funding for DOD's Biometric Program

Based on the figures provided by DOD as of November 2010, about $3.5 billion has been or will be spent to fund its biometrics programs from fiscal year 2007 through fiscal year 2015. DOD reports that almost two-thirds of the funding for its biometric program from fiscal year 2007 through fiscal year 2015 is drawn from the supplemental budget, which is in excess of DOD's base defense budget. Specifically, DOD reports that for fiscal years 2007 through 2011, supplemental funding accounts for over $2.0 billion for DOD's biometric programs with less than $500 million from defense base funding (see table 2).

Table 2: Biometric Program Funding, Fiscal Year 2007 through Fiscal Year 2011

Funding type (in millions)	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	Total funding FY 2007 through FY 2011
Base	$29.1	$52.0	$87.8	$134.3	$163.7	$466.9
Supplemental	347.7	442.3	499.2	528.7	606.0	2423.9
Total	**$376.8**	**$494.3**	**$587.0**	**$663.0**	**$769.7**	**$2890.8**

Source: GAO analysis of DOD documentation.

Note: This table reflects budget information provided as of November 2010 for DOD's biometrics program.

In contrast, in fiscal years 2012 through 2015 DOD is estimating base funding at more than $600 million, with no funding from supplements (see table 3). The change in funding, from supplemental support to base funding, is due in part to efforts to make a permanent program of record of DOD's biometric systems. DOD has begun to establish a more formal biometric program by identifying the requirements needed by the warfighter, assessing gaps in warfighting capabilities, and recommending solutions to resolve those gaps. DOD officials explain that as biometric technologies and systems become programs of records, funding should be built into base defense funding, rather than supplemental funding.

Table 3: Biometric Program Funding Fiscal Year 2012 through Fiscal Year 2015

Funding type (in millions)	FY 2012	FY 2013	FY 2014	FY 2015	Total funding FY 2012 through FY 2015
Base	$149.9	$178.2	$161.9	$175.9	$665.9
Supplemental	0.0	0.0	0.0	0.0	0.0
Total	**$149.9**	**$178.2**	**$161.9**	**$175.9**	**$665.9**

Source: GAO analysis of DOD documentation.

Note: This table reflects budget information provided as of November 2010 for DOD's biometrics program. Potential supplemental budget amounts for future years are not reflected in this table.

As shown, table 2 includes fiscal year 2007 through and including fiscal year 2011, and identifies biometric program base and supplemental funding while table 3 sets out fiscal year 2012 through fiscal year 2015, where it is currently unknown whether supplemental funding for the biometrics program will be requested.

We have previously recommended that DOD shift certain contingency costs into the annual base budget to allow for prioritization and trade-offs among its needs and to enhance visibility in defense spending.[1] With regard to its biometric program, DOD fiscal year 2012 through fiscal year 2015 budget plans shift funding into the base defense budget; however, DOD officials told us they anticipate continued need for supplemental funding to support the war efforts, but were unable to provide an estimate. As DOD identifies the warfighter needs related to developing future biometric capabilities, these requirements will likely affect its future budget requests.

[1]GAO, *Global War on Terrorism: DOD Needs to Take Action to Encourage Fiscal Discipline and Optimize the Use of Tools Intended to Improve GWOT Cost Reporting*, GAO-08-68 (Washington, D.C.: Nov. 6, 2007).

Appendix III: Comments from the Department of Defense

ASSISTANT SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

MAR 24 2011

Ms. Davi M. D'Agostino
Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. D'Agostino:

This is the Department of Defense (DoD) response to the GAO draft report 11-276, "DEFENSE BIOMETRICS: DoD Can Better Conform to Standards and Share Biometric Information with Federal Agencies," dated February 14, 2011 (GAO Code 351424). Detailed comments on the report recommendations are enclosed.

The Department concurs that adherence to technical interoperability standards for all biometric equipment, including verification devices, contributes to successful data sharing within the DoD and across the interagency. Additionally, the DoD remains committed to establishing and enforcing biometric data standards; and, since the time of the research for this GAO report, DoD has taken further steps to improve standards compliance testing. These steps have included the establishment of a Biometrics Standards Conformity Assessment Test Program that was accredited in January 2011 by the National Institute of Standards and Technology (NIST). The Department is also updating the existing authorities and responsibilities for standards testing in the DoD Directive 8521.01E, "Department of Defense Biometrics" to further strengthen our interoperability.

The Department also concurs with the need to look forward to the future data sharing requirements of our interagency partners, and to continually update our biometric database's ability to keep pace with those requirements as they evolve. DoD is actively engaged with the Department of Homeland Security, the Federal Bureau of Investigation, and other government departments and agencies on the steps required to achieve and maintain full interoperability.

Sincerely,

Zachary J. Lemnios

Enclosure:
As stated

GAO Draft Report Dated February 14. 2011
GAO-11-276 (GAO CODE 351424)

"DEFENSE BIOMETRICS: DOD CAN BETTER CONFORM TO STANDARDS AND SHARE BIOMETRIC INFORMATION WITH FEDERAL AGENCIES."

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Acquisition, Technology, and Logistics, as the Principal Staff Assistant responsible for the oversight of DOD biometrics, to take action in collaboration with other key federal agencies and internal DOD stakeholders, including BIMA, U.S. Army, U.S. Navy, U.S. Marines, and U.S. Air Force to implement a process for updating collection devices to adopted standards to help ensure that all DOD systems related to biometrics, including collection devices, conform to adopted standards. (See page 28/GAO Draft Report.)

DOD RESPONSE: Concur. The legacy HIIDE verification devices are approaching the end of their service life and are being retired, and DoD is in the process of procuring an updated handheld device to replace the HIIDE. The solicitation requires the replacement device to be compliant with the mandated data standard, which was EBTS 1.2 at the time the solicitation was developed and published, as required by DOD Directive 8521.01E for all new acquisitions. The Department expects to award this contract in April 2011, with fielding in August 2011. The Department's Biometrics Standards Conformity Assessment Test Program will verify compliance before deployment, and a separate engineering contract is already in place to upgrade devices to the recently-adopted EBTS 2.0 to ensure compatibility with interagency partners.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Acquisition, Technology, and Logistics, as the Principal Staff Assistant responsible for the oversight of DOD biometrics, to take action in collaboration with other key federal agencies and internal DOD stakeholders, including BIMA, U.S. Army, U.S. Navy, U.S. Marines, and U.S. Air Force to implement a process for testing collection devices at a sufficiently detailed level to help ensure that all DOD systems related to biometrics, including collection devices, conform to adopted standards. (See page 28/GAO Draft Report.)

DOD RESPONSE: Concur. The Department has established a Biometrics Standards Conformity Assessment Test Program, accredited in January 2011 as part of the National Institute of Standards and Technology's (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) for biometric testing. Relevant tests include conformance tests to DoD EBTS and FBI Electronic Fingerprint Transmission Specification, as well as evaluations and assessments of biometric-enabled devices and systems that interoperate with the authoritative biometrics database and other repositories of biometric data. While the current DoDD 8521.01E already requires such compliance testing for new biometrics acquisitions, the directive does not fully address quick reaction capabilities such as the HIIDE. Additionally, the Department will work with the Federal Bureau of Investigation to develop a co-sharing arrangement to leverage existing standards compliance testing at the FBI Biometric Center of Excellence to further strengthen interagency interoperability. The Department will update the Biometrics DoDD to include these requirements no later than September 2011.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Acquisition, Technology, and Logistics, as the Principal Staff Assistant responsible for the oversight of DOD biometrics, to take action in collaboration with other key federal agencies and internal DOD stakeholders, including BIMA, U.S. Army, U.S. Navy, U.S. Marines, and U.S. Air Force to more fully define and further clarify the roles and responsibilities needed to achieve DOD's biometric program and objectives for all stakeholders that include ensuring collection devices conform to adopted standards. (See page 28/GAO Draft Report.)

DOD RESPONSE: Concur. The Department is updating DoD Directive 8521.01E "Defense Biometrics," which establishes policy, assigns responsibilities, and describes procedures for DoD biometrics. This update will more fully define and clarify the roles and responsibilities of biometrics stakeholders, including responsibilities for testing collection devices for compliance with adopted standards. This update will be completed by September 2011.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Acquisition, Technology, and Logistics, as the Principal Staff Assistant responsible for the oversight of DOD biometrics, to take action in collaboration with other key federal agencies and internal DOD stakeholders, including BIMA, U.S. Army, U.S. Navy, U.S. Marines, and U.S. Air Force to complete the memorandum of agreement with the Department of Homeland Security regarding the sharing of biometric information as appropriate and consistent with U.S. laws and regulations and international agreements, as well as information sharing environment efforts. (See page 28/GAO Draft Report.)

DOD RESPONSE: Concur. The Memorandum of Agreement between DoD and DHS regarding biometric sharing was signed into effect on 03 March 2011.

RECOMMENDATION 5: The GAO recommends that the Under Secretary of Defense for Acquisition, Technology, and Logistics, as the Principal Staff Assistant responsible for the oversight of DOD biometrics, to take action in collaboration with other key federal agencies and internal DOD stakeholders, including BIMA, U.S. Army, U.S. Navy, U.S. Marines, and U.S. Air Force to identify its long-term biometric system capability needs, including the technological capacity and associated costs needed to support both the warfighter and to facilitate sharing of biometric information across federal agencies, and to take steps to meet those capability needs, as appropriate and consistent with U.S. laws and regulations, international agreements, and available resources. (See page 28/GAO Draft Report.)

DOD RESPONSE: Concur. DoD ABIS is currently meeting all the sharing transactions required by DHS and FBI, and the Department has expansion plans in place to grow ABIS's capability to over 40,000 daily transactions. This growth will meet the 14,000 daily biometrics transaction rate articulated by DHS for 2012. DoD continues to work closely with the interagency Interoperability Executive Steering Committee to ensure the DoD has visibility as new interagency requirements coalesce, and can modify ABIS expansion plans to be responsive to our interagency sharing responsibilities. The Department expects to have an updated ABIS sizing plan to support the projected future DoD and interagency transaction requirements by July 2011.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Davi M. D'Agostino, (202) 512-5431 or dagostinod@gao.gov

Acknowledgments

In addition to the contact named above, Penney Harwell Caramia, Assistant Director; Rebekah Boone; John Clary; Grace Coleman; Michele Fejfar; Lori Kmetz; Katherine Lenane; Amber Lopez Roberts; Greg Marchand; Jennifer Neer; Maria Stattel; Amie Steele; and Sonja Ware made key contributions to this report.

Related GAO Products

Homeland Security: Key US-VISIT Components at Varying Stages of Completion, but Integrated and Reliable Schedule Needed. GAO-10-13. Washington, D.C.: November 19, 2009.

Defense Management: DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing. GAO-09-49. Washington, D.C.: October 15, 2008.

Defense Management: DOD Needs to Establish Clear Goals and Objectives, Guidance, and a Designated Budget to Manage Its Biometrics Activities. GAO-08-1065. Washington, D.C.: September 26, 2008.

Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress. GAO-08-492. Washington, D.C.: June 25, 2008.

Homeland Security: Strategic Solution for US-VISIT Program Needs to be Better Defined, Justified, and Coordinated. GAO-08-361. Washington, D.C.: February 29, 2008.

GAO Management Letter to the Secretary of Defense. Washington, D.C.: December 13, 2007.

Terrorist Watch List Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List. GAO-08-110. Washington, D.C.: October 11, 2007.

Border Security: Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use. GAO-07-1006. Washington, D.C.: July 31, 2007.

Border Security: Strengthened Visa Process Would Benefit from Improvements in Staffing and Information Sharing. GAO 05-859. Washington, D.C.: September 13, 2005.

Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program. GAO-05-106. Washington D.C.: December 10, 2004.

Border Security: Joint, Coordinated Actions by State and DHS Needed to Guide Biometric Visas and Related Programs. GAO-04-1080T. Washington, D.C.: September 9, 2004.

Border Security: State Department Rollout of Biometric Visas on Schedule, but Guidance is Lagging. GAO-04-1001. Washington, D.C.: September 9, 2004.

Technology Assessment: Using Biometrics for Border Security. GAO-03-174. Washington, D.C.: November 15, 2002.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper