United States Government Accountability Office

GAO

Report to Congressional Committees

October 2008

DEFENSE MANAGEMENT

DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing

GAO-09-49

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Management. DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**33**	

October 2008

DEFENSE MANAGEMENT

DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-49, a report to Congressional Committees

Why GAO Did This Study

The events of September 11, 2001, and operations in Afghanistan and Iraq have made it critical for military units to identify individuals they encounter and share this information with other units and federal agencies. Biometrics are unique personal aspects such as fingerprints and iris images used to identify an unfamiliar person. Federal agencies with national security missions, such as the Departments of Homeland Security (DHS) and State (DOS), need access to certain biometrics data gathered by the Department of Defense (DOD). GAO was asked to determine to what extent (1) DOD has guidance on the biometrics data to be collected to support military activities, and (2) there may be gaps in biometrics information shared between DOD and DHS. This is a public version of a For Official Use Only report, GAO-08-430NI, issued in May 2008. GAO examined DOD's guidance for field collection of biometrics data, biometrics sharing agreements, and information on national level efforts to enhance data sharing.

What GAO Recommends

GAO recommends that (1) DOD establish guidance specifying a standard set of biometrics data for collection during military operations in the field, and (2) the Secretaries of Defense and Homeland Security address, as appropriate, biometrics data sharing gaps, in accordance with U.S. and international law. DOD partially concurred with the first recommendation and concurred with the second recommendation.

To view the full product, including the scope and methodology, click on GAO-09-49.
For more information, contact Davi D'Agostino at (202) 512-5431 or dagostinod@gao.gov.

What GAO Found

DOD has issued guidance on the biometrics data collected from individuals who are detained or allowed access to U.S. bases in Iraq, but has not issued guidance on data to be collected during field activities where U.S. forces encounter hostile or questionable individuals such as in Afghanistan and Iraq. DOD has allowed commanders to determine the type of data to collect, such as fingerprints or iris images, during their operations. GAO's analysis showed that allowing for this flexibility results in the collection of different data that are not necessarily comparable to each other. Some units may collect iris images while others collect fingerprints, which are not comparable data. Broader national security implications can arise, such as military personnel's inability to identify someone who has harmed or attempted to harm U.S. or coalition forces. These newly collected data are not necessarily comparable with data collected by other units or with federal databases that store biometrics data, such as the FBI's fingerprint database, DOD's biometric database, or the DHS biometric database. Having a standard set of data would help ensure consistent identification and confirmation of an individual's identity thus allowing forces to compare data across multiple databases in different commands. A standard set of data also would allow for comparison of new biometrics data collected in the field with existing biometrics data.

DOD shares biometrics data that it collects on non-U.S. persons with other federal agencies through a variety of inter-agency agreements, but some gaps in data sharing may remain. Since the events of September 11, 2001, the President and Congress have issued policies that require agencies to share counterterrorism information, and agencies have in turn issued their own policies. National efforts to develop policies about such information sharing are still in development. In January 2007, the Deputy Secretary of Defense issued a memo that stated that DOD would immediately adopt the practice of sharing, when asked, unclassified DOD biometrics data records with other U.S. agencies that have counterterrorism missions—this includes data related to terrorism information but excludes data pertaining to U.S. persons. According to a DHS memorandum, DHS is not regularly receiving updates on certain types of DOD biometrics data that it could use. DHS officials told GAO they could use such data in various ways, such as to prohibit individuals from entering the United States who are determined to be inadmissible based on these data and other relevant information. GAO found that DHS officials are consulting with DOD on how to obtain additional biometrics data from DOD. Until national level policies are developed, opportunities to reduce gaps in national security through comprehensive data sharing may be lost unless remaining needs for biometrics data are identified and filled as appropriate and in accordance with U.S. laws and regulations and international agreements.

Contents

Abbreviations

ABIS	Automated Biometric Identification System (DOD)
DHS	Department of Homeland Security
DOD	Department of Defense
DOS	Department of State
FBI	Federal Bureau of Investigation
IAFIS	Integrated Automated Fingerprint Identification System
IDENT	Automated Biometric Identification System (DHS)
US-VISIT	U.S. Visitor and Immigration Status Indicator Technology Office

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 15, 2008

The Honorable Solomon P. Ortiz
Chairman
The Honorable J. Randy Forbes
Ranking Member
Subcommittee on Readiness
Committee on Armed Services
House of Representatives

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Subcommittee on Terrorism and Unconventional Threats
and Capabilities
Committee on Armed Services
House of Representatives

The events of September 11, 2001, and operations to defeat insurgents in Afghanistan and Iraq have made it increasingly critical for military units to identify individuals they encounter in the field[1] and share this information with other units and certain federal agencies. Biometrics—measurements of unique personal characteristics, such as fingerprints,[2] irises,[3] and faces,[4] to identify an unfamiliar person—have become an important tool in these

[1]For the purposes of this report, "in the field" refers to military activities that take place in combat zones, like Iraq and Afghanistan, outside of U.S. bases and facilities. Specifically, this includes what DOD refers to as screening activities.

[2]Fingerprint identification is the method of identification using the impressions made by the minute ridge formations or patterns found on the fingertips.

[3]Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris, which is the muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye.

[4]According to the March 2007 *Report of the Defense Science Board Task Force on Defense Biometrics*, (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, March 2007), facial recognition is a convenient biometric because it is one of the few that is identifiable by both machines and humans, so it is generally used for identification cards and badges, although it should generally be used in combination with other biometrics.

operations, as well as in the Department of Defense's (DOD) business functions and military activities. For example, DOD uses biometrics to verify its common credential and to support access controls. In military activities, DOD uses biometrics to identify[5] and verify[6] individuals encountered in the field as friend, foe, or neutral; to operate detention facilities; to protect DOD personnel at expeditionary bases in theater (force protection); and to recover and identify U.S. personnel in Afghanistan and Iraq. Army and Marine Corps forces currently collect biometrics data (fingerprints, iris scans, and facial images) from (1) persons seeking access to U.S. installations in Iraq and Afghanistan, (2) detainees,[7] and (3) persons encountered by U.S. forces during military operations. Latent fingerprints are also recovered in combat zones from unknown individuals who may be foes or neutral.

Several DOD organizations are involved in developing guidance on the collection and use of biometrics data. The Secretary of Defense 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 her responsible for developing guidance for collecting and processing biometrics data. Additionally, DOD appointed the Director, Defense Research and Engineering, as the Principal Staff Assistant for Biometrics. The Director has developed and issued a biometrics directive identifying organizational roles and authorities for managing biometrics data.

Biometrics data, and the sharing of these data among federal agencies, are important to the United States' broader national security mission beyond DOD's operations in Afghanistan and Iraq. Homeland Security Presidential Directive 6, issued in September 2003, states that it is the policy of the United States to develop, integrate, and maintain terrorist information, and to use that terrorist information as appropriate and to the full extent

[5]Identification is the one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the known identity of the biometric subject whose template was matched.

[6]Verification is the one-to-one process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed to determine whether it matches the enrollee's template.

[7]Detainees are persons in the custody of DOD as a result of military operations.

permitted by law to support certain screening and other processes, including military, intelligence, law enforcement, immigration, and visa processes. In accordance with this and other laws and regulations, DOD, the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Department of State (DOS)[8] share biometrics information. The Intelligence Reform and Terrorism Prevention Act[9] 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. Additionally, the National Science and Technology Council, part of the Executive Office of the President, has created a subcommittee to address the use of biometrics across the federal government.

Within DOD, the Deputy Secretary of Defense, in a January 2007 memorandum, stated that DOD would immediately adopt the practice of sharing unclassified DOD biometrics data with other U.S. departments and agencies with counterterrorism missions. According to the memorandum, this includes data related to terrorism information defined in the Intelligence Reform and Terrorism Prevention Act[10] regarding terrorists, detainees, and those individuals or groups posing a threat to the United States, U.S. persons, or U.S. interests, but excludes data pertaining to U.S. persons, defined as U.S. citizens and aliens lawfully admitted for permanent residence. Non-U.S. persons are individuals who are neither U.S. citizens nor aliens lawfully admitted into the United States for permanent residence. The memorandum further states that sharing unclassified biometrics data unrelated to terrorism information will be determined based upon relevant law and directives but will require, at a minimum, a written memorandum from a requesting agency stating the official need for the data, the intended use of the data, the protections and safeguards that will be afforded the data, and the nature or extent of possible further distribution of the data to other organizations or agencies. Further, the memorandum stated that sharing of biometrics data on an

[8]The FBI and DHS each maintain their own biometrics databases. DHS's U.S.-Visitor and Immigrant Status Indicator Technology Office (US-VISIT) is responsible for DHS's biometrics database. DOS uses DHS's biometrics database in addition to its own database.

[9]The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, § 1016 (2004), codified as amended at 6 U.S.C. § 485.

[10]The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, § 1016(a)(4) (2004).

individual must be conducted pursuant to U.S. law and regulations and international agreements where appropriate.

The federal government currently does not maintain a comprehensive, governmentwide, biometrics-based terrorist database or watch list. In the absence of such a database or watch list and to increase the utility of the biometrics data it collects, DOD has established relationships—both with its own components and with interagency and multinational partners—through which it can share standardized biometrics files, analyses, and associated information in order to match results and determine whether there is a link between an individual's biometrics file and available associated information. Gaps in DOD's and other agencies' biometrics collection and sharing processes can increase the risk that terrorists will avoid identification in subsequent encounters with U.S. personnel during military operations, the visa application process, and U.S. border crossings. For example, during the visa application process or at a U.S. entry point, if terrorists are not identified as such, U.S. personnel may unknowingly grant them access to the United States.

While a number of biometrics databases exist across the federal government, there are three major federal biometrics databases that include, among other data sets, information on known and suspected terrorists:[11] (1) the FBI's Integrated Automated Fingerprint Identification System (IAFIS); (2) DOD's Automated Biometric Identification System (ABIS), which is collocated with IAFIS; and (3) the DHS Automated Biometric Identification System (IDENT), which is used by DHS for border patrol, customs, naturalization, and counterterrorism activities, as well as by DOS as part of its visa approval process.[12] DOD, the FBI, DHS, and DOS have established formal and informal arrangements, pursuant to applicable U.S. laws and regulations and international agreements, regarding the sharing of information among the IAFIS, ABIS, and IDENT databases.

[11]Other federal government databases containing terrorist-related information include the National Counterterrorism Center's Terrorist Identities Datamart Environment and the Terrorist Screening Center's database. Though these databases contain and search against biographical information, they do not search against biometrics data. However, the federal government is working toward including biometrics information on known and suspected terrorists in the national database maintained by the Terrorist Screening Center.

[12]DOS uses DHS's biometrics database in addition to its own database.

At your request, we reviewed and reported on DOD's strategic efforts to manage identity information, including biometrics data, which is used for a variety of purposes, such as to identify individuals seeking access to bases.[13] In the course of this work, we identified collection and sharing issues that we brought to your attention in a version of this report that was designated For Official Use Only and issued in May 2008.[14] This following report is the public version of that report, GAO-08-430NI. As our May 2008 report contained information that DOD considered sensitive and designated For Official Use Only, this version of the report omits references and information pertaining to detailed collection guidance and sensitive database information, including an appendix. We have indicated those changes with footnotes within the report. Our objectives in this report were to determine to what extent (1) DOD has guidance that establishes the biometrics data to be collected to support military activities and (2) there may be gaps in biometrics information shared between DOD and DHS. To answer the first objective, we examined DOD's policies and procedures for the collection of biometrics data during field operations. We also interviewed DOD officials from Marine Corps Headquarters, the Army's Biometrics Task Force, the National Ground Intelligence Center, U.S. Central Command, and U.S. Special Operations Command. To determine the extent to which there may be gaps in biometrics information sharing between DOD and DHS, we reviewed available interagency biometrics data-sharing agreements and held discussions with officials from DOD, DOS, the FBI, and DHS's U.S.-Visitor and Immigrant Status Indicator Technology (US-VISIT) program office.[15] We focused our work in this area on DOD, DOS, the FBI, and US-VISIT because of the biometrics database locations and sharing relationship among the databases. We included other federal agencies that use DOD-collected biometrics in carrying out their own national security missions. Because DOD viewed some aspects of the report as sensitive and designated them For Official Use Only, and because other information was classified, some details of our evidence could not be discussed in this report. We conducted this performance audit from May 2007 to May 2008

[13]GAO, *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.: Sept. 28, 2008).

[14]GAO, *Defense Management: DOD Needs to Establish More Guidance for Biometrics Collection and Explore Broadening Data Sharing*, GAO-08-430NI (Washington, D.C.: May 21, 2008).

[15]US-VISIT administers DHS's IDENT on behalf of all of DHS.

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. A full description of our scope and methodology can be found in appendix I.

Results in Brief

DOD has issued guidance specifying the biometrics data to be collected on individuals who are detained or allowed access to U.S. bases in Iraq, but has not issued guidance specifying a standard set of data to be collected during field activities. In 2000, DOD established the Biometrics Task Force to provide guidance on the collection of biometrics data. In recognizing the different conditions commanders may encounter in the field, DOD has allowed commanders to determine the type of biometrics data to collect during their operations. However, we determined that allowing for this flexibility results in the collection of different data that are not necessarily comparable to each other. For example, some units may collect iris images while others collect fingerprints, which are not comparable data. Broader national security implications can arise from the collection of incomparable data, such as military personnel's inability to identify someone who has harmed or attempted to harm U.S. or coalition forces. These newly collected data would not necessarily be comparable with data collected by other units or with large federal databases that store biometrics data, such as the FBI's fingerprint database and DOD's biometrics database. For example, iris image data collected by military units are not comparable with the FBI's fingerprint database. Thus, iris-only screenings cannot be used to identify these individuals. Similarly, biometrics files that include only iris images cannot be used to match latent fingerprints, which are often collected in combat zones. Having a standard set of biometrics data would help ensure consistent identification and confirmation of an individual's identity thus allowing forces to compare data across multiple databases in different commands and to determine whether individuals should be detained. A standard set of data would also allow for comparison of new biometrics data collected in the field with existing biometrics data. Therefore, we recommend that the Secretary of Defense direct the Secretary of the Army's Executive Manager for Biometrics to establish guidance specifying a minimum baseline standard set of biometrics data for collection during military operations in the field so that biometrics data can be compared across multiple databases in different commands and across federal agencies as

appropriate and in accordance with U.S. laws and regulations and international agreements.

DOD shares biometrics data that it collects on non-U.S. persons[16] with other federal agencies through a variety of interagency agreements, but some gaps in data sharing may remain. For example, according to a 2007 DHS memorandum, there are certain types of DOD biometrics data that DHS is not receiving updates of on a routine basis. DHS officials told us they could use such biometrics data in various ways, such as to prohibit individuals from entering the United States who are determined to be inadmissible based on these data and other relevant information, to detain individuals for law enforcement reasons, or to provide DHS additional information about refugees and their potential eligibility to enter the United States. The DHS memorandum also states that DHS was consulting with DOD on how to obtain additional biometrics data from DOD. However, DHS officials stated that to date the only progress has been the sharing of Iraqi asylum and refugee data, which provides DHS with biometrics data on individuals that DOD has encountered in Iraq. The National Science and Technology Council has several efforts under way to develop national policies and procedures to better coordinate the use of biometrics data among agencies. Also, the Program Manager for the Information Sharing Environment is to plan and oversee the implementation of the information sharing environment, among other duties. For example, the Program Manager for the Information Sharing Environment is involved with the National Science and Technology Council's efforts.[17] However, until such national-level policies are developed and implemented, opportunities to fill or reduce gaps in our national security through comprehensive data sharing may be lost unless remaining needs for biometrics data are appropriately filled. We recommend that until a formalized, governmentwide biometrics data-sharing architecture is implemented, the Secretaries of Defense and Homeland Security, in consultation with other federal agencies, such as the FBI and DOS, determine if biometrics information sharing needs are being met and address, as appropriate, any biometrics data-sharing gaps that may exist, in accordance with U.S. laws and regulations and

[16]In some cases, DOD cannot be certain if the fingerprints are from a non-U.S. person.

[17]Officials from the office of the Program Manager for the Information Sharing Environment stated that they have made efforts to incorporate biometrics into future versions of various biometrics standards, including standards efforts for Terrorist Watch listing with the Terrorist Screening Center and the National Counterterrorism Center.

international agreements, as well as Information Sharing Environment efforts.

In commenting on a draft of this report, DOD partially concurred with our recommendation that the Secretary of Defense direct the Biometrics Task Force to establish guidance specifying a standard set of biometrics data for collection during military operations in the field. DOD stated that if our recommendation to establish this guidance was directed at DOD personnel in stable environments—not field environments—then DOD fully agreed with our recommendation and would take action to implement it. However, DOD commented that if we were referring to collection in field environments, DOD officials still wanted to rely on commanders' judgment about what data to collect. We disagree and continue to believe that DOD should establish guidance on the collection of a minimum baseline standard set of biometrics data when collecting biometrics data during military activities in the field, or what DOD refers to as screening operations, as has been done in Afghanistan, to mitigate the risks we identified and DOD acknowledged. DOD concurred with our recommendation to determine if biometrics information sharing needs are being met and if there are any gaps in sharing that may exist. In its comments, DOD stated that it is fully participating in and fully supportive of interagency forums specifically chartered to address improved sharing of biometrics data and interoperability of biometrics systems. DOD's written comments are reprinted in appendix II.

Background

As the technologies for collecting, storing, and sharing biometrics data advance, DOD and other federal agencies that collect, use, store, and share such data in the conduct of their national security missions have expanded their biometrics efforts. DOD uses biometrics for various purposes—including controlling access to DOD facilities, intelligence analysis,[18] and identifying and verifying non-U.S. persons encountered during field activities in Afghanistan and Iraq. U.S. forces collect, match, and share biometrics data, and DOD has developed a number of policies and procedures to govern these activities. However, guidance for the collection and use of biometrics data is still evolving.

[18]The Army's National Ground Intelligence Center has a mission to produce intelligence to support the U.S. forces on the battlefield. This currently includes analysis of matches of biometrics data and the maintenance of a watch list for use by warfighters.

Governmentwide Policies Regarding Biometrics Data Are Evolving

Historically, the FBI has been the dominant federal government user of biometrics, with a long-established fingerprint database—IAFIS—as its primary biometrics data repository. Other federal agencies, like DHS and DOS, also use biometrics in support of their respective national security missions, including border patrol, customs, disaster recovery, naturalization, visa processes, and counterterrorism. DHS's US-VISIT program office administers IDENT on behalf of all of DHS. IDENT is the database DHS has designated as the central point for all of the department's biometrics collection, identification, and storage efforts. DOS has access to IDENT data via its sharing agreement with DHS for use in its visa screening process. To date, DOD and DHS have not established a direct link between their two biometrics databases and rely on the FBI's IAFIS database as an indirect link between DOD and DHS. This is a result of specific biometrics sharing agreements and other information sharing policies and agreements. If biometrics data for non-U.S. persons collected by DOD are not retained in the FBI's IAFIS, other agencies, like DHS and DOS, that send biometrics data for searching to IAFIS, do not have access to this DOD information when they conduct searches for visa, citizenship, border control, and other homeland security purposes. While limited occasional direct sharing of DOD and DHS biometrics has occurred, it is not regularized.

Several efforts are under way to develop national policies and procedures to better coordinate the use of biometrics data and to ensure that concerns such as privacy are addressed. For example, the National Science and Technology Council has established the Subcommittee on Biometrics and Identity Management to address issues such as identity management, privacy, and biometrics system improvements and to develop policy foundations for those issues.[19] In addition, the Information Sharing Environment Program Manager, in consultation with the Information Sharing Council, is to plan and oversee the implementation of and manage an Information Sharing Environment, an approach that facilities the sharing of terrorism and homeland security information. The Program Manager is also responsible for assisting, monitoring, and assessing the implementation of the Information Sharing Environment by federal

[19]To date, the National Science and Technology Council's Subcommittee on Biometrics and Identity Management states that it has published the following documents on biometrics: *The National Biometrics Challenge* (Washington, D.C.: August 2006); *NSTC Policy for Enabling the Development, Adoption, and Use of Biometric Standards* (Washington, D.C.: Sept. 7, 2007); and *Privacy and Biometrics: Building A Conceptual Foundation* (Washington, D.C.: Sept. 15, 2006).

departments and agencies to ensure adequate progress, technological consistency, and policy compliance, among other duties.

While these efforts are under way, many departments, including DOD, continue to collect biometrics data to meet their individual missions. However, even within departments, there may not be policies to ensure that officials in different parts of the organization are aware of or have access to biometrics data that are collected by others.

DOD Collection, Matching, and Sharing of Biometrics Data

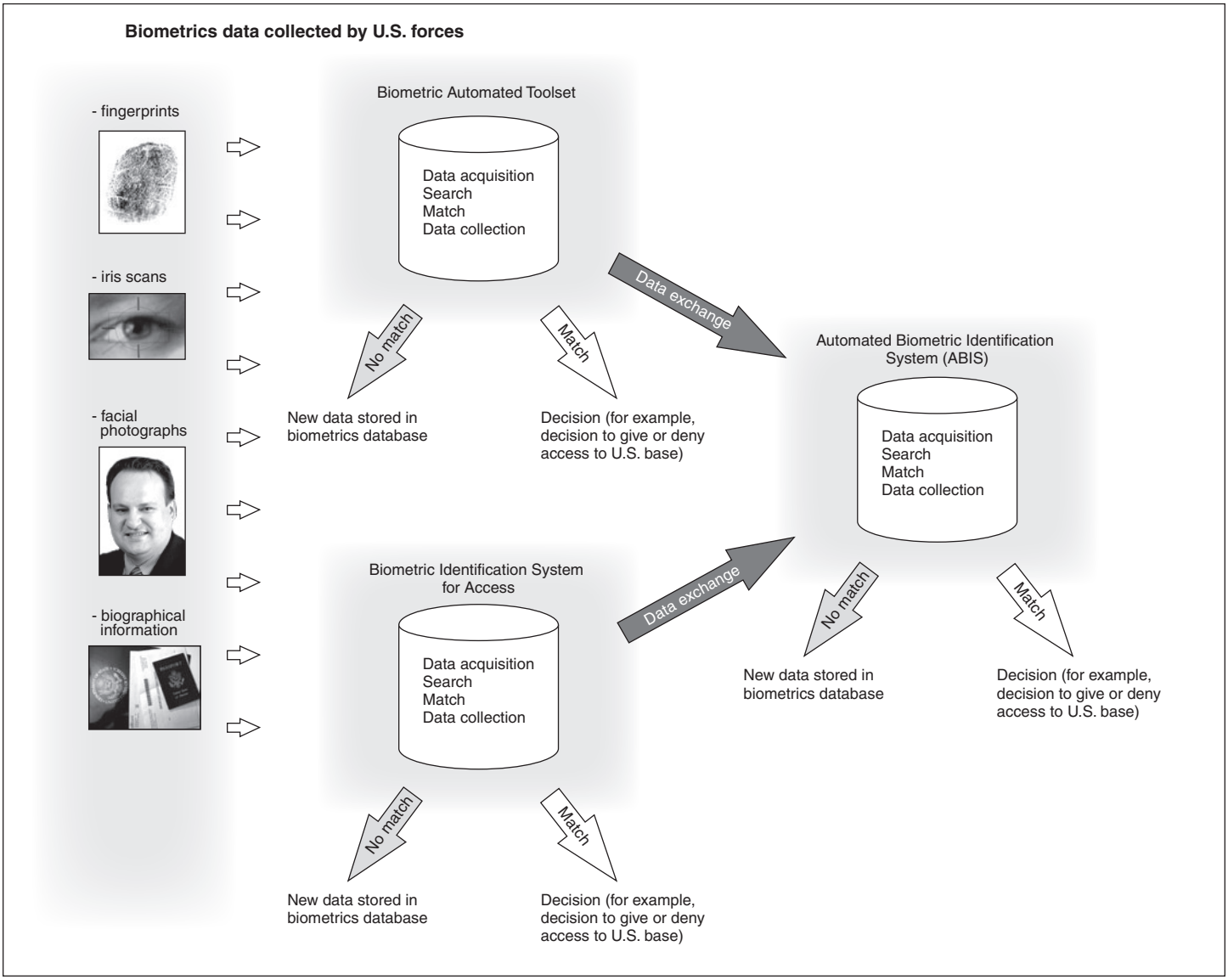
During DOD field activities, such as those in Afghanistan and Iraq, U.S. forces collect biometrics data for a variety of purposes, such as to control access to U.S. bases in order to protect personnel and to identify and verify non-U.S. persons that they encounter. The primary system for biometrics data collection in U.S. Central Command, including Afghanistan and Iraq, is the Biometric Automated Toolset. The Biometric Automated Toolset is a DOD biometrics system that allows U.S. forces to collect fingerprints, iris scans, facial photographs, and biographical information of persons of interest and store them in a searchable database. DOD has also established the Biometric Identification System for Access, which includes similar types of biometrics data but is limited to use on installations in Iraq to determine whether non-U.S. persons should have access to U.S. bases.

Once U.S. forces have collected the biometrics data, they attempt to compare and match the data to previously collected data stored in the Biometric Automated Toolset and the Biometric Identification System for Access. These data are also sent to ABIS[20]—the DOD-wide database for non-U.S. persons' biometrics—to determine if U.S. forces have previously encountered an individual and entered the individual's biometrics data into this database. If there is not a match, the new data are stored in the Biometric Automated Toolset and ABIS and maintained for future use, as appropriate. Figure 1 illustrates this process.[21]

[20]ABIS is DOD's electronic database and associated set of software applications that support the storage, retrieval, and searching of multiple types of biometric data collected from persons of national security interest. Over time, DOD plans for ABIS to incorporate functionality to support the storage, retrieval, and searching of additional biometric modalities such as face images, iris images, and voice print samples. ABIS shares the same fundamental design, and is collocated, with the FBI's IAFIS.

[21]A brief paragraph noting some of the biometrics information included in ABIS was removed because DOD designated such information For Official Use Only.

Figure 1: DOD Biometrics Data Collection and Sharing



Sources: GAO analysis of DOD data, Corbis (fingerprint), and GAO (iris, facial photograph, and documents).

Once biometrics data are in ABIS, they can be shared or sent to another biometrics database, such as the FBI's IAFIS, for additional matching attempts against non-DOD records. DOD has established agreements with the FBI and DHS that allow it to share its biometrics data with them, both to assist DOD in identifying the individuals it encounters during its military

activities and to inform other federal agencies of DOD's interactions with non-U.S. persons who might be of interest. For example, DOD uses the Biometric Identification System for Access to collect biometrics from a non-U.S. person seeking access to a U.S. facility in Iraq and sends that information back to DOD's ABIS database to see if the new data match any biometrics data currently stored in ABIS. While ABIS is being searched, DOD forwards the biometrics data to the FBI's IAFIS database to see if there is a U.S. criminal history for the individual seeking access to U.S. facilities in Iraq. Once the FBI conducts its search, it sends the results back to DOD and does not keep noncriminal biometrics data collected using the Biometric Identification System for Access. In other cases, for example, when an individual is detained in Iraq or Afghanistan by DOD, the process is the same until DOD sends the biometrics data to the FBI. In most of these cases, the FBI stores the biometrics data in IAFIS, a criminal database, for potential future use.

During field activities, DOD personnel collecting biometrics data may not know if the person is a non-U.S. person until the data are collected and then matched with already existing data. For example, DOD personnel collecting latent fingerprints during and after combat operations may not know until the fingerprints are matched with existing data if the person is a non-U.S. person.

DOD Has Issued Limited Guidance for Collecting Biometrics Data

The Biometrics Task Force has not issued guidance specifying a standard set of biometrics data that would allow for comparison of newly collected biometrics data with existing biometrics data in the field. Having a standard set of biometrics data would help ensure consistent identification and confirmation of an individual's identity thus allowing forces to compare data across multiple databases in different commands and to determine whether individuals should be detained. In recognition of the conditions commanders face in the field, DOD delegated responsibility to field commanders to determine the type of biometrics data personnel should collect during their operations. As a result, some units may collect fingerprints and facial photos, while others may collect only iris images, even though they are all using devices that can collect the same types of biometrics. For example, Marine Corps units prefer to collect iris scans during field identification and verification activities, but Special Operations Forces and Army units in other parts of Iraq prefer to collect

fingerprints in the field—typically a minimum of two index finger prints and two thumb prints.[22]

The lack of comparable data also has implications for broader national security issues. For example, military personnel may be unable to identify someone who has harmed or attempted to harm U.S. or coalition forces. The collection of similar or baseline data by DOD and departments or agencies involved in national security activities, such as counterterrorism, could enable them to use the same biometrics data across a wide range of national security missions. Given the lack of comparability of the new data collected in the field, such as when a unit collects exclusively iris images, the data would not match against records in larger federal databases, such as the FBI's IAFIS. If these data could be compared to such databases, this capability would help the unit determine with certainty whether these individuals had been encountered before and whether they should be detained.[23] For example, biometrics files that include only iris images cannot be used to match latent fingerprints collected in combat zones. Thus, military personnel collecting only iris images may be unable to identify someone who has harmed or attempted to harm U.S. or coalition forces.

DOD and other federal agency officials said that there can be a trade-off between tactical (warfighter) needs—for example, the necessity when operating in a hostile environment to perform tasks expeditiously to reduce the risk of bodily harm—and strategic (national security) needs—for example, the ability of intelligence analysts to make connections among individuals, groups, and events, or the use of data for counterterrorism and border security in the United States. Thus, localized discretion about what types of biometrics data to collect may enable DOD personnel to conduct quick and efficient screenings under potentially hostile conditions, but the data they collect may be of little use to both military units in the field and other U.S. government entities in support of future counterterrorism efforts, including border security. Agencies both within and outside of DOD—the National Ground Intelligence Center, U.S. Central Command, U.S. Special Operations Command, the Biometrics Fusion Center, and the FBI—acknowledge that without a baseline national

[22]A sentence regarding a Marine Corps report was removed because DOD designated such information For Official Use Only.

[23]An example regarding a terrorist watch list was removed because DOD designated such information For Official Use Only.

standard for biometrics collection that maximizes the utility of the data both for the warfighters in the field and for national security efforts at home, opportunities to identify persons of interest may be lost.

DOD Shares Data on Non-U.S. Persons through Interagency Agreements, but Some Gaps in Data May Remain

DOD shares biometrics data that it collects on non-U.S. persons with other federal agencies through a variety of interagency agreements, but some gaps in data sharing may remain. Despite the sharing agreements, a DHS memorandum indicates that DHS does not regularly receive certain types of data from DOD. DHS officials stated that this information could potentially be used to carry out DHS's national security mission. DOS officials also believe such data could be used to support DOS's visa processing mission. To date, the only regular progress has been the sharing of Iraqi asylum and refugee data, which provide DHS with biometrics data on individuals that DOD has encountered in Iraq.

Since the events of September 11, 2001, the President and Congress have issued broad policies that require federal agencies to share counterterrorism information, and federal agencies have in turn issued their own policies. A January 2007 Deputy Secretary of Defense memorandum called for DOD to immediately adopt the practice of sharing unclassified DOD biometrics data records with other U.S. departments and agencies that have counterterrorism missions, including data related to terrorism information defined in the Intelligence Reform and Terrorism Prevention Act regarding terrorists, detainees, and those individuals or groups posing a threat to the United States, U.S. persons, or U.S. interests, but excluding data pertaining to U.S. persons, defined as U.S. citizens and aliens lawfully admitted for permanent residence. The memorandum also specified that the sharing of biometrics data records on an individual must be conducted in accordance with U.S. laws and regulations and international agreements.[24] This memorandum was issued pursuant to Homeland Security Presidential Directive 6, Homeland Security Presidential Directive 11,[25] an interagency memorandum of understanding

[24]Also in January 2007, the Deputy Secretary of Defense issued another memorandum authorizing combatant commanders to share DOD-collected biometrics records (excluding those pertaining to U.S. persons) with coalition partners and other allies as required to meet mission requirements.

[25]Homeland Security Presidential Directive 11, issued in 2004, builds upon Homeland Security Presidential Directive 6, issued in 2003, and states that it is the policy of the United States to implement a coordinated and comprehensive approach to the collection, analysis, dissemination, and use of information related to certain threats to the United States. It states that agencies should build upon existing systems and best practices.

agreeing to support the Terrorism Screening Center,[26] and the Intelligence Reform and Terrorism Prevention Act of 2004—all federal policies that encourage the sharing of terrorism information. Also, the Intelligence Reform and Terrorism Prevention Act of 2004 directed the President to, among other things, create an Information Sharing Environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties. The act further stated that the President shall ensure that the Information Sharing Environment provides and facilitates the means for sharing terrorism information among all appropriate federal, state, local, and tribal entities and the private sector through the use of policy guidelines and technologies. To the greatest extent practicable, the President shall ensure that the Information Sharing Environment, among other things, connects and builds upon existing systems capabilities in use across the government, where appropriate; allows users to share information among agencies, between levels of government, and as appropriate with the private sector; and facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations, and operations. The act also created a Program Manager to plan and oversee the implementation of the Information Sharing Environment, among other responsibilities. Additionally, the National Science and Technology Council has several efforts under way to develop national policies and procedures to better coordinate the use of biometrics data among federal agencies.

According to DOD's January 2007 memorandum, sharing unclassified DOD biometrics data with other U.S. departments and agencies with counterterrorism missions includes data related to terrorism information defined in the Intelligence Reform and Terrorism Prevention Act regarding terrorists, detainees, and those individuals or groups posing a threat to the United States, U.S. persons, or U.S. interests, but excludes data pertaining to U.S. persons, defined as U.S. citizens and aliens lawfully admitted for permanent residence. The memorandum further states that the sharing of unclassified biometrics data unrelated to terrorism information will be determined based upon relevant law and directives and will require, at a minimum, a written memorandum from a requesting agency stating the official need for the data, the intended use of the data, the protections and

[26]The original memorandum of understanding on the integration and use of biometrics screening was signed in 2003 by DOS, the Department of Justice, and DHS as well as the intelligence community. The agreement was updated in 2004 to include DOD and the Department of the Treasury.

safeguards that will be afforded the data, and the nature or extent of possible further distribution of the data to other organizations or agencies. Further, the memorandum states that sharing of biometrics data on an individual must be conducted pursuant to U.S. law and regulations and international agreements where appropriate.

DOD and other federal agencies involved in national security operations share biometrics data through a variety of agreements that have evolved on a case-by-case basis. However, a 2007 DHS memorandum indicates that the department is not receiving frequent updates on some DOD biometrics data. DHS officials said that the department could use these data for national security purposes. According to an April 2007 DHS memorandum, certain categories of information that DHS is not receiving frequent updates on include information from DOD's Biometric Automated Toolset. According to DHS officials, DHS does not have a sharing agreement with DOD regarding[27] these data, and such an agreement could allow DHS to update its database on a routine basis. Because DHS obtained the data from DOD as a one time event through the FBI, it received only the data that existed at that 2006 date. Additionally, the DHS memorandum states that DHS does not have access to DOD's Biometric Identification System for Access, a noncriminal database. While DOD sends Biometric Identification System for Access data to the FBI for potential matches, the FBI does not retain this noncriminal information. According to FBI officials, DHS has sharing agreements with the FBI, but in this case, since the FBI told us that it does not retain the DOD data and DHS does not have an agreement with DOD, DHS does not receive the data. Lastly, the DHS memorandum states that DHS receives latent fingerprint images from various sources under Operation Iraqi Freedom and Operation Enduring Freedom as part of the larger set of all latent prints associated with the FBI's Unsolved Latent File—latent fingerprints that have not been linked to an identity. However, the memorandum further states that DHS has requested that DOD submit latent fingerprints separately to better provide awareness of any possible subsequent DOD-specific latent fingerprint identifications.

According to the April 2007 DHS memorandum, DHS was discussing how it could obtain additional biometrics data from DOD. According to DHS, these data could be used to (1) prohibit individuals from entering the

[27]The names of certain data sets were removed because DOD designated such information For Official Use Only.

United States who are determined to be inadmissible based on these data and other relevant information, (2) detain individuals for law enforcement reasons if needed, or (3) provide additional information about refugees and their potential eligibility to enter the United States. DHS officials further stated that the department could receive some of the DOD data through the FBI, if the FBI retained it, or if DHS had a specific data-sharing agreement with DOD. The DHS memorandum states that DHS will continue to engage DOD regarding the sharing of additional biometrics data. However, DHS officials stated that to date the only progress has been the sharing of Iraqi asylum and refugee data, which provides DHS with biometrics data on individuals that DOD has encountered in Iraq.[28] DOS officials stated that they also could potentially use DOD's Biometric Identification System for Access data. According to DOS officials, these data could assist DOS in verifying that a non-U.S. person has legitimately accessed U.S. facilities in Iraq.

Conclusion

If DOD does not have a standard set of biometrics data for use in the field, then it will be unable to determine whether the individuals its forces encounter in the field are friend, foe, or neutral and will therefore possibly endanger its forces. Moreover, until comprehensive information sharing agreements are worked out or the National Science and Technology Council develops and implements a national architecture for biometrics data collection, in consultation with information sharing environment efforts, biometrics information collected by U.S. forces from individuals encountered in the field may not be fully utilized by other federal agencies for national security activities. For example, the sharing of latent fingerprints collected by DOD personnel in combat zones could potentially help enable a DOS consular official to deny a visa to an individual who attacked U.S. forces in Iraq. Opportunities to reduce gaps in our security through comprehensive data sharing may be lost unless remaining needs for biometrics data are appropriately filled. Because potential harm could come to U.S. interests from those individuals DHS and DOS could have prevented from entering the United States—if those individuals were determined to be inadmissible based on these data and other relevant information—it is important that DOD, the FBI, DHS, and DOS work

[28]According to DHS, progress to that end has included development of a draft data-sharing agreement between DHS and DOD for the regularized sharing of actionable biometrics. Additionally, Iraqi individuals applying for DHS asylum or refugee status are periodically searched against DOD biometrics data.

together to determine the biometrics data needed and to share these data in accordance with applicable laws, regulations, and international treaties.

Recommendations for Executive Action

We recommend that the Secretary of Defense direct the Secretary of the Army's Executive Manager for Biometrics to establish guidance specifying a minimum baseline standard set of biometrics data for collection during military operations in the field so that biometrics data can be compared across multiple databases in different commands and across federal agencies as appropriate and in accordance with U.S. laws and regulations and international agreements.

Additionally, we recommend that until a formalized, governmentwide biometrics data-sharing architecture is implemented, the Secretaries of Defense and Homeland Security, in consultation with other federal agencies, such as the FBI and DOS, determine if biometrics information sharing needs are being met and address, as appropriate, any biometrics data-sharing gaps that may exist, in accordance with U.S. laws and regulations and international agreements, as well as information sharing environment efforts.

Agency Comments and Our Evaluation

We requested comments on a For Official Use Only draft of this report from the Executive Office of the President's National Science and Technology Council; DOD; DOS; DHS; the FBI; the Program Manager, Information Sharing Environment; and the Office of the Director of National Intelligence's National Counterterrorism Center. DOD was the only agency to provide written comments on the For Official Use Only version of this report. As such, this public version of the For Official Use Only report was sent to DOD for comment. DOD partially concurred with our recommendation to establish guidance specifying a standard set of biometrics data for collection during military operations in the field. In comments, DOD stated that if our recommendation to establish this guidance was directed at DOD personnel in stable environments—not field environments—then DOD fully agreed with our recommendation and would take action to implement it. However, DOD commented that if we were referring to collection in field environments, DOD officials still wanted to rely on commanders' judgment as to what to collect. In our recommendation, we referred to collection of biometrics during military operations in the field, which we equate to DOD's screening operations of suspicious or potentially hostile individuals, which could include biometrics collection in hostile environments. Our point was that if one unit collected one type of biometrics, such as an iris scan from an

individual, and another unit later collected fingerprints from the same individual, no match could be made between the two different encounters of the individual and potential persons of interest could be released. Moreover, DOD acknowledges this risk in its comments, stating that DOD officials want to continue to rely on the commanders' judgment on the biometrics to be collected during military operations in the field, including hostile environments. However, we continue to believe that DOD should establish guidance for a minimum baseline biometrics collection standard to mitigate this risk, especially since guidance in place in Afghanistan, a hostile area of operations, already establishes such a minimum. A DOD document[29] sets forth the procedures for standardization of mandatory fields that must be completed during the collection processes for various biometrics collection systems. Collecting biometrics data above and beyond such a minimum baseline standard could be left up to the commander's discretion; however, we continue to believe that a minimum biometrics collection requirement for military operations in the field, or what DOD calls screening operations, should be established, as was done for Afghanistan operations, to mitigate the risks we identified and DOD acknowledged in its comments. Based on DOD's comments on the For Official Use Only draft report, we revised this recommendation and the final report to reflect the appropriate office responsible for this guidance and to clarify that we intend for DOD to establish a minimum standard for biometrics data collected from individuals encountered during military operations in the field.

DOD concurred with our recommendation to determine if biometrics information sharing needs are being met and if there are any gaps in sharing that may exist. In its comments, DOD stated that it is fully participating in and fully supportive of interagency forums specifically chartered to address improved sharing of biometrics data and interoperability of biometrics systems.

The Executive Office of the President's National Science and Technology Council; DOD; DHS; the Program Manager, Information Sharing Environment; and the Office of the Director of National Intelligence's National Counterterrorism Center provided technical comments on the For Official Use Only version of this report, which we have incorporated into this report as appropriate.

[29]Specific information about this document was removed because DOD designated such information For Official Use Only.

DOD's written comments are reprinted in appendix II.

As agreed with your offices, we are sending copies of this report to the Chairman and Ranking Member of the House Committee on Armed Services and other interested congressional parties. We are also sending copies of this report to the Secretary of Defense; the Secretary of State; the Attorney General of the United States; the Secretary of Homeland Security; the Executive Office of the President's Office of Science and Technology Policy, National Science and Technology Council; the Director, the Federal Bureau of Investigation; the Director, National Counterterrorism Center; and the Program Manager, Information Sharing Environment, Office of the Director of National Intelligence.

If you or your staff have any questions concerning this report, please contact me at (202) 512-5431 or dagostinod@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Davi M. D'Agostino
Director
Defense Capabilities and Management

Appendix I: Scope and Methodology

Scope

We focused the scope of our work on the Department of Defense (DOD), the four military services (Army, Navy, Marine Corps, and Air Force), the Department of State (DOS), the Department of Homeland Security's (DHS) U.S.-Visitor and Immigrant Status Indicator Technology (US-VISIT) program office, and the Department of Justice's Federal Bureau of Investigation (FBI). Federal agencies outside of DOD were included because of their use of DOD-collected biometrics as part of their national security portfolios, and we reviewed their use of biometrics inasmuch as it relates to the biometrics information collected by DOD and shared with other agencies. Any other information gathered regarding federal agencies outside of DOD was strictly for background purposes. Because DOD viewed some aspects of the report as sensitive and designated them For Official Use Only, and because other information was classified, some details of our evidence could not be discussed in this report.

Methodology

To determine the processes and procedures under which DOD is collecting biometrics data for military operations, we reviewed DOD-wide and service-specific directives, memorandums, concepts of operations, and standard operating procedures. To develop background on the collection of biometrics data by DOD, we analyzed information published by GAO, DOD, the Defense Science Board, and the Executive Office of the President's National Science and Technology Council. We reviewed documents from and obtained the perspectives of officials in relevant DOD commands and agencies throughout the department and the military services, as listed in table 1. The documents and meetings with officials allowed us to obtain an integrated understanding of how DOD uses biometrics, specifically for military operations such as detainee management, force protection, and identifying individuals during combat operations.

Table 1: Installations and Offices Where GAO Obtained Documentary Evidence and Officials' Views Pertaining to Defense Biometrics

Service	Installation or office
DOD	Joint Staff J34, Operations Directorate, Antiterrorism and Homeland Defense
	Joint Staff J8, Force Structure Resources and Assessment
	Director, Defense Research and Engineering
	DOD Chief Information Officer
	U.S. Central Command
	U.S. Special Operations Command
	U.S. Joint Forces Command
Army	Biometrics Task Force
	Program Executive Office, Enterprise Information Systems, Program Manager, Biometrics
	Biometrics Fusion Center
	Headquarters, Department of the Army, Deputy Chief of Staff for Intelligence (G-2)
	National Ground Intelligence Center
Navy	Office of the Secretary of the Navy
Marine Corps	Headquarters U.S. Marine Corps, Plans, Policies, and Operations, Force Protection Branch, Security Division
	Headquarters U.S. Marine Corps, Command, Control, Communications, and Computers
	Marine Corps Systems Command

Source: GAO.

To assess the extent to which biometrics data collected by DOD are shared with other federal agencies, we met with and reviewed documents from officials at DOD and the federal agencies listed in table 2.

Table 2: Non-DOD and Interagency Offices Where GAO Obtained Documentary Evidence and Officials' Views Pertaining to Defense Biometrics

Agency	Installation or office
Interagency	Technical Support Working Group
Executive Office of the President	National Science and Technology Council, Subcommittee on Biometrics and Identity Management
Department of State	Consular Affairs
	Diplomatic Security
Department of Justice	Federal Bureau of Investigation, Criminal Justice Information Services
Department of Homeland Security	US-VISIT
Department of Commerce	National Institute of Standards and Technology

Source: GAO.

The documents and meetings with officials allowed us to obtain an integrated understanding of how biometrics collected by DOD are shared with other federal agencies with national security (specifically counterterrorism) missions. To determine the processes and procedures under which DOD is sharing biometrics and related information with other federal agencies, we reviewed DOD-wide and service-specific directives, memorandums, and interagency agreements, as well as relevant agreements between other federal agencies, such as the FBI and US-VISIT. We also gathered and reviewed documentation regarding the information sharing environment and the National Science and Technology Council.

We conducted this performance audit from May 2007 to May 2008 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: Comments from the Department of Defense

Note: Page numbers in the draft report may differ from those in this report.

DIRECTOR OF DEFENSE RESEARCH AND ENGINEERING
3030 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-3030

OCT 3 2008

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, GAO-09-49, "DEFENSE MANAGEMENT: DoD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing," dated September 22, 2008 (GAO Code 351261). Detail comments on the report recommendations are enclosed.

The Department concurs that the collection of standardized biometric modalities for biometric enrollments is critical to our ability to compare data and reliably identify individuals who pose a threat. Since the time of the research for this report, DoD has established additional guidance to standardize the biometric modalities collected during enrollments, but continues to maintain that screening procedures, vice enrollment, must be conducted in consideration of the tactical environment as determined by the Commander.

The Department fully supports more robust sharing of biometric and biographic data with other agencies, including the Department of Homeland Security (DHS), to the extent that it is conducted in full compliance of the laws pertaining to the protection of privacy and personal identifying information, and is actively pursuing more formal arrangements for doing so with DHS and other government departments and agencies.

Sincerely,

Alan R. Shaffer
Principal Deputy

Enclosure:
As stated

GAO DRAFT REPORT – DATED SEPTEMBER 22, 2008
GAO CODE 351261/GAO-09-49

"DEFENSE MANAGEMENT: DoD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Secretary of the Army's Executive Manager for Biometrics to establish guidance specifying a minimum baseline standard set of biometrics data for collection during military operations in the field so that biometrics data can be compared across multiple databases in different commands and across Federal agencies as appropriate and in accordance with U.S. laws and regulations and international agreements. (Page 19/GAO Draft Report)

DOD RESPONSE: Partially Concur.

GAO clearly identifies the risk associated with inconsistent collection of biometrics modalities. Different biometric modalities cannot be matched to one another (eg., an iris image cannot be matched to a fingerprint) and attempts to screen target individuals by using a modality that is not stored and available within the watch-list will necessarily fail. In recognition of this risk, policy has been developed and promulgated to guide the collection of biometrics. In March 2005, the Army Biometrics Task Force, acting on behalf of the DoD Executive Agent for Biometrics, published a Standard Operating Procedure that identified the three modalities that should be collected whenever possible. Additionally U.S. Central Command and its components have issued policies that specify collection requirements, including which biometric modalities are to be collected, during enrollment.

In all cases, this published guidance includes the requirement to collect fingerprints, iris images and facial images when enrolling a person into the Automated Biometric Identification System (ABIS) and the Biometric Automated Toolset (BAT). Not all encounters in the field, however, result in the enrollment of a person into the biometrics repositories. In many cases, persons who are not suspected of causing, or intending to cause, harm to U.S. interests are simply screened against the DoD biometrics watchlist when encountered. Screening can be accomplished by comparing any

biometric modality against that same modality that is resident within our watchlist. So long as the watchlist contains all modalities, there is no need to screen multiple modalities for each person encountered. The risk of not screening against all modalities contained within the watchlist for every encounter must be weighed by the Commander in the context of his tactical mission requirements. Should the tactical operators have reason to suspect the person of intending harm to U.S. interests, however, he will be enrolled and full biometrics will be collected thereby ensuring that future encounters can be matched against any biometric. To the extent that GAO recommends collection of full modalities for biometric enrollments, DoD fully concurs with the recommendation and will take additional steps to promulgate such policy. Screening procedures, however, must be conducted in consideration of the tactical environment as determined by the Commander.

RECOMMENDATION 2: The GAO recommends that, until a formalized, Government-wide, biometrics data-sharing architecture is implemented, the Secretaries of Defense and Homeland Security, in consultation with other Federal agencies, such as the Federal Bureau of Investigation and the Department of State, determine if biometrics information sharing needs are being met and address, as appropriate, any biometrics data sharing gaps that may exist, in accordance with U.S. laws and regulations and international agreements, as well as information sharing environment efforts. (Page 19/GAO Draft Report)

DOD RESPONSE: Concur.

The ongoing conflicts in Iraq and Afghanistan have given DoD an unprecedented opportunity to collect biometric and biographical data on persons encountered overseas who intend harm to U.S. interests. DoD has developed and actively maintains a robust biometrically enabled watchlist that allows DoD commanders to vet persons encountered in the field or seeking access to U.S. facilities or positions of trust. The success of this watch-listing process, which begins with data collection in the field and includes the data storage and matching capability, has led to the detention of hundreds of adversaries. As GAO properly states, the data that has enabled DoD successes in the forward operating theaters is equally relevant to other federal agencies charged with screening for persons who present a threat to the U.S. DoD fully supports more robust sharing of biometric and biographic data with other agencies, including the Department of Homeland Security (DHS), to the extent that it is conducted in full compliance of the laws pertaining to the protection of privacy and personal identifying information. To that end, as recognized in the GAO report, in January 2007 the Deputy Secretary of Defense promulgated guidance directing all DoD components to immediately begin sharing all unclassified biometric data with other U.S. Departments and Agencies having a counter-terrorism mission.

As correctly stated in the GAO report, DoD has made its full repository of non-US person biometrics, ABIS, available real-time to the FBI Criminal Justice Information Services (CJIS) division. More relevant than the full DoD biometric database, however, is the DoD biometrically enabled watchlist that contains the biometric records of those individuals known to present a threat to the U.S. and our coalition partners. This watch-list is also provided to the FBI and has been made available to the Department of Homeland Security. In July 2007 DoD provided its full watchlist, all tiers, to the Dept of Homeland Security and is in active discussions with DHS concerning the establishment of a formal sharing agreement. Additionally, DoD makes available the full contextual background of persons contained on the DoD biometrically enabled watchlist available to all federal agencies with Secret Internet Protocol Router (SIPR) or Joint Worldwide Intelligence Communications System (JWICS) access and the lawful need to know.

In addition to bilateral efforts to improve biometric related data sharing among the federal agencies, DoD is fully participating in and fully supportive of interagency forums specifically chartered to address improved sharing of biometrics data and interoperability of biometrics systems. Among these bodies are the National Science and Technology Council Subcommittee on Biometrics and Identity Management and the Department of Justice led interagency working group that is drafting the implementation guidance for National Security Presidential Directive-59 / Homeland Security Presidential Directive-24. Although bi-lateral arrangements between DoD and the various agencies provide a short-term mechanism for sharing relevant biometric data, the strategic solution to the sharing issue is being developed within these groups.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contacts

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

Acknowledgments

In addition to the contact named above, Lorelei St James, Assistant Director; Bethann Ritter; David Artadi; Brian Kime; Joanne Landesman; Katherine Lenane; John Nelson; and Karen Werner made key contributions to this report.