

September 2008

DEFENSE MANAGEMENT

DOD Needs to Establish Clear Goals and Objectives, Guidance, and a Designated Budget to Manage Its Biometrics Activities





Highlights of [GAO-08-1065](#), a report to congressional requesters

Why GAO Did This Study

The Department of Defense (DOD), in its response to unconventional threats from terrorists, uses biometrics technologies that identify physical attributes, including fingerprints and iris scans. However, coordinating the development and implementation of biometrics and ensuring interoperability across DOD has been difficult to achieve.

Biometrics also is an enabling technology for identity management, a concept that seeks to manage personally identifiable information to enable improved governmentwide sharing and analysis of identity information. GAO was asked to examine the extent to which DOD has established biometrics goals and objectives, implementing guidance for managing biometrics activities, and a designated budget. To address these objectives, GAO reviewed documentation, including DOD biometrics policy and directives, and interviewed key DOD officials involved with making policy and funding decisions regarding biometrics.

What GAO Recommends

To improve DOD's management of its biometrics activities, GAO recommends that the Secretary of Defense ensure that the Principal Staff Assistant and Executive Committee establish clear goals and objectives, implementing guidance, and a designated budget for managing its biometrics activities. DOD concurred with all of GAO's recommendations.

To view the full product, including the scope and methodology, click on [GAO-08-1065](#). For more information, contact Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov.

DEFENSE MANAGEMENT

DOD Needs to Establish Clear Goals and Objectives, Guidance, and a Designated Budget to Manage Its Biometrics Activities

What GAO Found

DOD established, in October 2006, the Principal Staff Assistant, who is the Director of Defense Research and Engineering, and an Executive Committee as part of its attempts to improve the management of its biometrics activities. However, as of August 2008, it had not established management practices that include clearly defined goals and objectives, implementing guidance that clarifies decision-making procedures for the Executive Committee, and a designated biometrics budget. First, while DOD has stated some general goals for biometrics, such as providing recognized leadership and comprehensive planning policy, it has not articulated specific program objectives, the steps needed to achieve those objectives, and the priorities, milestones, and performance measures needed to gauge results. Second, DOD issued a directive in 2008 to establish biometrics policy and assigned general responsibilities to the Executive Committee and the Principal Staff Assistant but has not issued implementing guidance that clarifies decision-making procedures. The Executive Committee is chaired by the Principal Staff Assistant and includes a wide array of representatives from DOD communities such as intelligence, acquisitions, networks and information integration, personnel, and policy and the military services. The Executive Committee is responsible for resolving biometrics management issues, such as issues between the military services and joint interests resulting in duplications of effort. However, the committee does not have guidance for making decisions that can resolve management issues. Past DOD reports have noted difficulties in decision making and accountability in the management of its biometrics activities. Third, DOD also has not established a designated budget for biometrics that links resources to specific objectives and provides a consolidated view of the resources devoted to biometrics activities. Instead, it has relied on initiative-by-initiative requests for supplemental funding, which may not provide a predictable stream of funding for biometrics.

Prior GAO work on performance management demonstrates that successful programs incorporate such key management practices, and for several years, DOD reports and studies have also called for DOD to establish such practices for its biometrics activities. Similarly, a new presidential directive issued in June 2008 supports the establishment of these practices in addition to calling for a governmentwide framework for the sharing of biometrics data. DOD officials have said that DOD's focus has been on quickly fielding biometrics systems and maximizing existing systems to address immediate warfighting needs in Afghanistan and Iraq. This focus on responding to immediate warfighting needs and the absence of the essential management practices have contributed to operational inefficiencies in managing DOD's biometrics activities, such as DOD's difficulties in sharing biometrics data within and outside the department. For example, in May 2008 GAO recommended that DOD establish guidance specifying a standard set of biometrics data for collection during military operations in the field. These shortcomings may also impede DOD's implementation of the June 2008 presidential directive and the overall identity management operating concept.

Contents

| | | |
|---------------------|--|-----------|
| Letter | | 1 |
| | Results in Brief | 5 |
| | Background | 7 |
| | DOD Biometrics Lacks Clear Goals and Objectives, Implementing Guidance, and a Designated Budget | 10 |
| | Conclusions | 19 |
| | Recommendations for Executive Action | 20 |
| | Agency Comments and Our Evaluation | 20 |
| Appendix I | Scope and Methodology | 23 |
| Appendix II | DOD Actions to Improve Coordination of Biometrics | 25 |
| Appendix III | GAO Management Letter to the Secretary of Defense | 27 |
| Appendix IV | DOD Response to GAO Management Letter | 32 |
| Appendix V | Comments from the Department of Defense | 34 |
| Appendix VI | GAO Contact and Staff Acknowledgments | 37 |
| Figures | | |
| | Figure 1: Key DOD Actions Related to Management of Biometrics Activities | 9 |
| | Figure 2: Key DOD Entities Involved in Biometrics Activities | 14 |

This is a work of the U.S. government and is not subject to copyright protection in the United States. It 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.



United States Government Accountability Office
Washington, DC 20548

September 26, 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 U.S. security environment has changed markedly in recent years. Once focused on the Cold War threat of the Soviet Union with its massive conventional forces and nuclear arsenal, the Department of Defense (DOD) now faces not only potential conventional threats from hostile nations but also unconventional threats from terrorist organizations or individuals. For example, these terrorists may seek to blunt U.S. forces by blending anonymously into native populations to avoid detection until an attack is launched. DOD uses fingerprint records, iris scans, and other biometrics technologies to help establish the identity of such persons. Biometrics technologies can be useful because they measure physical attributes of individuals, such as the whorls, arches, and furrows of their fingerprints or the random patterns of the iris muscle of the eye, which are thought to be unique to an individual. Biometrics data not only can help establish a person's identity with greater confidence but also help improve the ability to link individuals to their past activities and previously used

identities.¹ According to DOD, biometrics technology is revolutionizing DOD operations and is used in many organizations and in many missions, including military operations such as population control, counterintelligence screening, and detainee management and interrogation, and in business operations such as base access control to verify Common Access Card credentials.²

Biometrics activities are dispersed throughout DOD at many organizational levels. These DOD organizations use a variety of different systems to collect, store, and analyze biometrics data. However, with many organizations developing the use of biometrics, coordination has been difficult to achieve across the department, according to several DOD reports. DOD efforts to formally organize and manage its biometrics activities date back to at least 2000 when Congress designated the U.S. Army as the Executive Agent responsible for leading and coordinating all DOD biometrics information assurance programs. Given current wartime missions following the terrorist attacks on September 11, 2001, DOD has spent millions of dollars in procuring biometrics technologies and systems and installing them throughout the department and in its operations overseas. For example, for fiscal years 2006 and 2007, the Army alone received approval for about \$540 million in biometrics-related funding and requested over \$470 million in funding for fiscal year 2008. With the increased use of biometrics, DOD recognized that it needed to establish better overarching direction for its biometrics activities and improve coordination among the DOD organizations involved, and began to institute various initiatives to achieve those goals. For example, by memorandum dated October 4, 2006, the Deputy Secretary of Defense designated the Director of Defense Research and Engineering, under the Under Secretary of Defense for Acquisition, Technology and Logistics, as the Principal Staff Assistant for DOD Biometrics. The Deputy Secretary directed the Principal Staff Assistant to establish the DOD Biometrics

¹While biometrics technologies have advanced security operations, they have limitations. For example, some people working extensively at manual labor may have fingerprints too worn to be recorded. In addition, errors may also occur during matching operations. For this reason some security systems may use multiple biometrics to increase their accuracy. For a more detailed examination of biometrics accuracy rates, see GAO, *Technology Assessment: Using Biometrics for Border Security*, [GAO-03-174](#) (Washington, D.C.: Nov. 15, 2002).

²In 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.

Executive Committee (Executive Committee) with members representing DOD's military services and intelligence, acquisitions, networks and information integration, personnel, and policy communities. In a February 2008 directive, DOD designated the Principal Staff Assistant as the chair of the Executive Committee.

While biometrics technologies are important tools in DOD operations, they also are enabling technologies for the much broader operating concept termed identity management. While the definition for identity management is evolving, a basic understanding from federal and DOD reports and other documents is that identity management seeks to manage identity information, including biometrics data, in an integrated, coordinated way to enable improved sharing and analysis of identity information. Biometrics data represent only a part of an individual's identity. For example, in addition to unique physical attributes, such as fingerprints and iris scans, other information on individuals may include their names, Social Security numbers, or dates of birth. Identity information on known or suspected terrorists, as well as U.S. or foreign individuals, may also be collected, organized, analyzed, and protected in databases associated with military combat or base access operations or intelligence, law enforcement, border security, or other national security mission areas. The greater confidence provided by biometrics data raises the potential for it to be used as a "master key" to grant access across all these databases and systems, and cross-reference information from all the different perspectives—subject to existing privacy protections—resulting in the opportunity for new analytical perspectives. In its 2006 concept of operations,³ DOD recognized that its current methods of identifying individuals, organizing information on persons, and recalling and sharing such information were inadequate to meet its operational needs. As a result, DOD saw the need to integrate its dispersed biometrics operations to be consistent with the type of improved information sharing and analysis sought by identity management. The need for increased sharing of biometric and other information in the Global War on Terrorism is also being recognized across the federal government. For example, in June 2008, the President issued a new national security directive establishing a governmentwide framework for the sharing of biometrics data.⁴ The

³Department of Defense, *Capstone Concept of Operations for DOD Biometrics in Support of Identity Superiority* (Washington, D.C.: November 2006).

⁴The 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).

directive is designed to ensure that federal agencies use compatible methods and procedures in the collection, storage, use, and analysis of biometric information to enhance the sharing of such data.

In light of the increasing importance of biometrics and identity management to DOD's missions and the significant amount of funding devoted to biometrics technologies, you asked that we examine the effectiveness of DOD's efforts to manage biometrics in support of the larger context that is identity management. This is the third in a series of products we have issued in response to your request. In December 2007, we issued a management letter raising concerns about whether the newly established Principal Staff Assistant for Biometrics was being provided with the authority needed to improve coordination and direction of DOD's biometrics initiatives.⁵ In May 2008, we recommended that DOD establish guidance specifying a standard set of biometrics data for collection during military operations in the field, and explore broadening its data sharing with other federal agencies in some areas.⁶ In this report, we examine the extent to which DOD has established biometrics goals and objectives, implementing guidance for managing biometrics activities, and a designated budget linking resources to specific objectives and providing a consolidated view of the resources devoted to biometrics activities.

To address this report's objective, we considered leading management practices and principles identified in our prior reports and analyses.⁷ Our analysis focused primarily on DOD's management of biometrics activities, systems, and programs associated with its current warfighting and counterterrorism efforts, particularly those used in U.S. Central Command's geographic area of responsibility, which includes Iraq and Afghanistan. We reviewed documents and interviewed officials from a range of DOD organizations at the departmental, military service, and combatant command levels involved in conducting, managing, or

⁵Unnumbered letter to the Secretary of Defense dated December 13, 2007. See app. III.

⁶GAO, *Defense Management: DOD Needs to Establish More Guidance for Biometrics Collection and Can Explore Broadening Data Sharing*, [GAO-08-430NI](#) (Washington, D.C.: May 21, 2008).

⁷GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004); *Determining Performance and Accountability Challenges and High Risks*, [GAO-01-159SP](#) (Washington, D.C.: November 2000); and *Executive Guide: Effectively Implementing the Government Performance and Results Act*, [GAO/GGD-96-118](#) (Washington, D.C.: June 1996).

overseeing biometrics activities. These documents included various memorandums, directives, briefings, progress reports, budgetary data, planning documents, charters, agendas, reports, studies, and analyses related to biometrics activities in the department. To understand DOD's biometrics activities within a federal government context, we also obtained information and met with officials from other federal agencies and offices and reviewed the February 2008 National Security Presidential Directive on the use of biometrics to enhance national security. We conducted this performance audit from May 2007 through September 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. Further details on our scope and methodology can be found in appendix I.

Results in Brief

DOD began to take actions to better manage its dispersed biometrics activities in 2000, but as of August 2008, it had not established management practices that include clearly defined goals and objectives, implementing guidance that clarifies decision-making procedures for the Executive Committee, and a designated biometrics budget. First, while DOD has stated some general goals for biometrics, such as providing comprehensive planning policy in several documents such as the November 2005 *Department of Defense Biometrics Strategy*, it has not articulated specific program objectives, the steps needed to achieve those objectives, and the priorities, milestones, and performance measures needed to gauge results. DOD officials said that in late 2008 they plan to complete studies that will lay the foundation for the eventual development of a formal biometrics program. Second, DOD issued a directive in 2008 to establish biometrics policy and assigned general responsibilities to the Executive Committee and the Principal Staff Assistant but has not issued implementing guidance that clarifies decision-making procedures for policy and management issues. The Executive Committee is chaired by the Principal Staff Assistant and includes a wide array of representatives from DOD communities such as intelligence, acquisitions, networks and information integration, personnel, and policy and the military services. The Executive Committee is responsible for resolving biometrics management issues, such as issues between the military services and joint interests resulting in duplications of effort. However, the committee does not have guidance for making decisions that can resolve management issues. At one time, DOD considered providing the Executive Committee

with a voting mechanism to resolve policy issues and help ensure that such issues and others are formally addressed and resolved in the best interests of the department as a whole. However, this directive did not include this voting mechanism. Past DOD reports have noted difficulties in decision making and accountability in the management of its biometrics activities. Third, DOD also has not established a designated budget for biometrics that links resources to specific objectives and provides a consolidated view of the resources devoted to biometrics activities. Instead, it has relied on initiative-by-initiative requests for supplemental funding, which may not provide a predictable stream of funding for biometrics. Until DOD has established a designated budget, it will continue to experience uncertainty in obtaining resources for its biometrics activities.

Our prior work on performance management demonstrates that successful programs incorporate such key management practices, and for several years, DOD reports and studies have also called for DOD to establish such practices for its biometrics activities. Similarly, a new presidential directive issued in June 2008 supports the establishment of these practices in addition to calling for a governmentwide framework for the sharing of biometrics data. DOD officials have said that DOD's focus has been on quickly fielding biometrics systems and maximizing existing systems to address immediate warfighting needs in Afghanistan and Iraq. This focus on responding to immediate warfighting needs and the absence of the essential management practices have contributed to operational inefficiencies in managing DOD's biometrics activities, such as DOD's difficulties in sharing biometrics data within and outside the department. For example, in May 2008, we recommended that DOD establish guidance specifying a standard set of biometrics data for collection during military operations in the field. These shortcomings may also impede DOD's implementation of the June 2008 presidential directive and the overall identity management operating concept. Therefore, we are recommending that DOD establish clearly defined goals and objectives, issue implementing guidance that clarifies decision-making procedures for the Executive Committee, and establish a designated budget for managing its biometrics activities.

GAO provided a draft of this report to DOD in August 2008 for its review and comment. In written comments on the draft, DOD concurred with all of our recommendations. Also, the Director of Defense Biometrics provided us with technical comments, which we incorporated in the report where appropriate. DOD's response is reprinted in appendix V.

Background

DOD has been using biometrics since the 1970s, and with improvements in the technologies used to collect and share this information, DOD's use of biometrics has increased. As this use increased, reports have called on DOD to improve its management of biometrics activities and, over time, DOD has taken some key actions. Meanwhile, a new concept called identity management is emerging of which biometrics is an integral part.

Growing Use of Biometrics

The use of biometrics to authenticate a person's identity is not new. A method to index fingerprints was first developed in the late 1800s, and the U.S. prison system began using fingerprints to identify criminals in 1903. Additional forms of biometrics, such as facial and iris recognition, began being used in the latter half of the 20th century, but the emergence of computer systems to help automate the recognition process resulted in an explosion of activity in biometrics in the 1990s. DOD's involvement in biometrics dates back at least to the 1970s, but a 1999 initiative for DOD to move to the use of smart card technology as the principal mechanism for access to its buildings and databases set the stage for the increased use of biometrics in the department.⁸ With the wars in Afghanistan and Iraq, DOD and the military services expanded the use of biometrics for tactical military operations, such as helping identify known or suspected terrorists on the battlefield and controlling the movement of local civilian populations.

Reports to DOD on Management of Biometrics and DOD Actions

Several reports have called on DOD to improve its management of biometrics. For example, in the August 2005 *Joint Urgent Operational Need Statement for a Joint Biometrics Solution in Support of Operations*, U.S. Central Command reported that the "lack of a comprehensive management approach to the development and implementation of biometrics technology" was resulting in "unfocused investment" of resources with DOD services and agencies fielding individual systems with varying levels of interoperability, undercutting the command's operations in Iraq and Afghanistan. A second DOD report in 2006 identified a host of problems where biometrics systems were fielded without regard to an overarching design and often had different applications and capabilities with different data fields, resulting in a lack

⁸Deputy Secretary of Defense, Memorandum on Smart Card Adoption and Implementation (Washington, D.C.: Nov. 10, 1999). Smart cards are plastic devices about the size of a credit card that use integrated circuit chips to store and process data, much like a computer.

of interoperability and synchronization, and duplication of data.⁹ More recently, in March 2007, a report by the Defense Science Board Task Force on Defense Biometrics cited the “reactive” and “ad hoc” nature of DOD’s management of biometrics initiatives since the terrorist attacks of September 11, 2001.¹⁰

In July 2000, Congress designated the Secretary of the Army as the “Executive Agent to lead, consolidate, and coordinate all biometrics information assurance programs” across DOD.¹¹ Since then, DOD has taken various actions over time to address management of biometrics activities, as shown in figure 1. For example, DOD has formed at least three coordinating groups over the past 6 years to help improve coordination and management of its biometrics activities. DOD’s actions culminated in the February 2008 DOD Directive, which established general biometrics policy and organizational responsibilities, with the Principal Staff Assistant responsible for coordinating and overseeing biometrics and the Executive Committee, chaired by the Principal Staff Assistant, responsible for reviewing and approving biometrics strategy and program plans and for resolving biometrics issues and disputes. The directive calls for DOD to integrate biometrics into its operations, eliminate unwarranted duplication and overlap of efforts, and ensure that biometrics capabilities be developed to be interoperable with other identity management capabilities and systems.¹² Further information on DOD’s actions is included in appendix II.

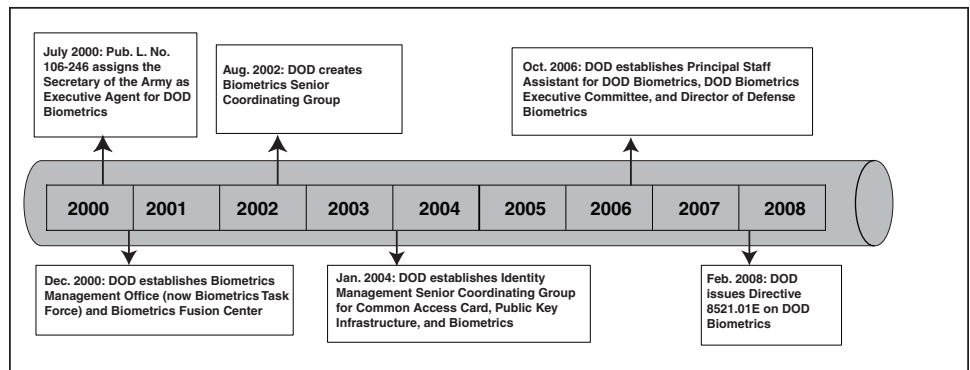
⁹Biometrics Tiger Team of the Executive Agent for DOD Biometrics, *Biometrics Tiger Team Trip Report 23 April – 5 May 2006* (Washington, D.C.: June 28, 2006).

¹⁰Defense Science Board, *Report of the Defense Science Board Task Force on Defense Biometrics* (Washington, D.C.: March 7, 2007). This report was requested by the Under Secretary of Defense for Acquisition, Technology and Logistics on April 13, 2006.

¹¹Pub. L. No. 106-246, § 112 (2000).

¹²Department of Defense Directive 8521.01E, *Department of Defense Biometrics* (Feb. 21, 2008).

Figure 1: Key DOD Actions Related to Management of Biometrics Activities



Source: GAO analysis of DOD documents.

Emerging Concept of Identity Management

As DOD's use of biometrics has expanded, recognition of the broader concept of identity management—generally understood as the management of personal identity information, including biometrics data, in an integrated, coordinated way to enable improved sharing and analysis of said information—has emerged within the department and the federal government. For example, in its March 2007 report on the use of biometrics within DOD, the Defense Science Board's Task Force on Defense Biometrics urged the department to “embrace the larger construct” of identity management, rather than focus solely on biometrics.¹³ Similarly, according to officials from the National Science and Technology Committee's Subcommittee on Biometrics and Identity Management within the Executive Office of the President, which is responsible for coordinating biometrics policy across the federal government, the subcommittee added “Identity Management” to its name in the spring of 2007 to reflect the increasingly broader nature of its activities.

In addition to being a key component of identity management, information sharing among federal agencies has also grown in importance for national security purposes. The overall U.S. national security establishment has been moving toward an increasingly interoperable, sharing approach to terrorism-related identity information in the wake of the intelligence

¹³Defense Science Board, *Report of the Defense Science Board Task Force on Defense Biometrics*.

failures associated with the terrorist attacks of September 11, 2001. For example, in 2004, Congress directed the President to establish a formal Information Sharing Environment program to facilitate the sharing of terrorist information. Since then, strategies and plans for developing an information-sharing architecture cutting across the entire federal government—including the intelligence, law enforcement, defense, homeland security, and foreign affairs communities—have been under development. This information includes not only biometrics identity data but virtually all information regarding terrorist organizations. According to Office of Science and Technology Policy officials who lead the National Science and Technology Council’s Subcommittee on Biometrics and Identity Management, they supported the development of the new presidential directive calling for broader sharing of biometrics data across the federal government, and are also working to develop additional interagency products for potential use in informing broader elements of a governmentwide policy foundation for biometrics.¹⁴

DOD Biometrics Lacks Clear Goals and Objectives, Implementing Guidance, and a Designated Budget

DOD has not established clearly defined goals and objectives, implementing guidance clarifying decision-making procedures for the Executive Committee, and a designated budget linking resources to specific objectives for its biometrics activities. Our prior work has found that such management practices are key to program success.¹⁵ First, although DOD has developed some general goals for biometrics, it has not articulated specific program objectives, the steps needed to achieve those objectives, and the priorities, milestones, and performance measures needed to gauge results. Second, DOD issued a directive in 2008 that, among other things, established biometrics policy and assigned general responsibilities to the Executive Committee, which is chaired by the Principal Staff Assistant. However, the department has not issued implementing guidance that clarifies the committee’s decision-making procedures for resolving policy differences among its members, who represent a wide range of DOD communities and the military services with different functional responsibilities or operational requirements for

¹⁴To date, the Subcommittee on Biometrics and Identity Management has published the following documents on biometrics: National Science and Technology Council Subcommittee on Biometrics and Identity Management, *The National Biometrics Challenge* (Washington, D.C.: August 2006); *NSTC Policy for Enabling the Development, Adoption, and Use of Biometrics Standards* (Washington, D.C.: Sept. 7, 2007); and *Privacy and Biometrics: Building a Conceptual Foundation* (Washington, D.C.: Sept. 15, 2006).

¹⁵See [GAO-04-408T](#), [GAO-01-159SP](#), and [GAO/GGD-96-118](#).

biometrics. Such guidance is important to help the Executive Committee ensure the interoperability of biometrics systems and prevent duplication of biometrics-related efforts within the department—problems that have affected DOD’s management of biometrics in the past. Third, DOD has not established a designated budget for biometrics that links resources to specific objectives or that provides a consolidated view of resources devoted to biometrics. Instead, the department has relied on initiative-by-initiative requests for supplemental funding for its biometrics activities, which may not provide a predictable stream of funding. Having a designated budget also helps to link resources to specific objectives and provides an organization with a consolidated view of specific activities.

DOD Biometrics Activities Lack Clear Goals and Objectives

DOD has not articulated clearly defined goals and objectives that would inform the development and implementation of biometrics activities for DOD and the services. Our prior work has found that management principles, such as providing a clear expression of goals and objectives, are key to program success.¹⁶ While DOD has developed a variety of concept papers and other documents discussing biometrics concepts and activities, as well as a number of tactical plans and documents discussing timelines for improvements to individual biometrics technologies and systems, these attempts do not provide sufficient management direction to help ensure program success. For example, the Biometrics Task Force published the *Department of Defense Biometrics Strategy* in November 2005, which lays out general goals and objectives. The strategy states goals such as providing “recognized leadership” and “comprehensive planning and policy.” However, these goals and objectives did not provide a clear expression of the specific program objectives, the steps needed to achieve those results, and the priorities, milestones, and performance measures needed to gauge results.

Similarly, the DOD *Capstone Concept of Operations for DOD Biometrics in Support of Identity Superiority* dated November 2006 also provides important concepts of the use of biometrics in both military operations and business functions. However, it is not a biometrics program plan with goals, timelines, and performance measures. Further, in September 2006, the Identity Protection and Management Senior Coordinating Group produced a draft *Roadmap to Identity Superiority*. This document provides a more specific strategic vision of biometrics and some

¹⁶See [GAO-04-408T](#), [GAO-01-159SP](#), and [GAO/GGD-96-118](#).

associated programs, including specific goals and expected timelines. However, DOD officials told us that the document has not been finalized.

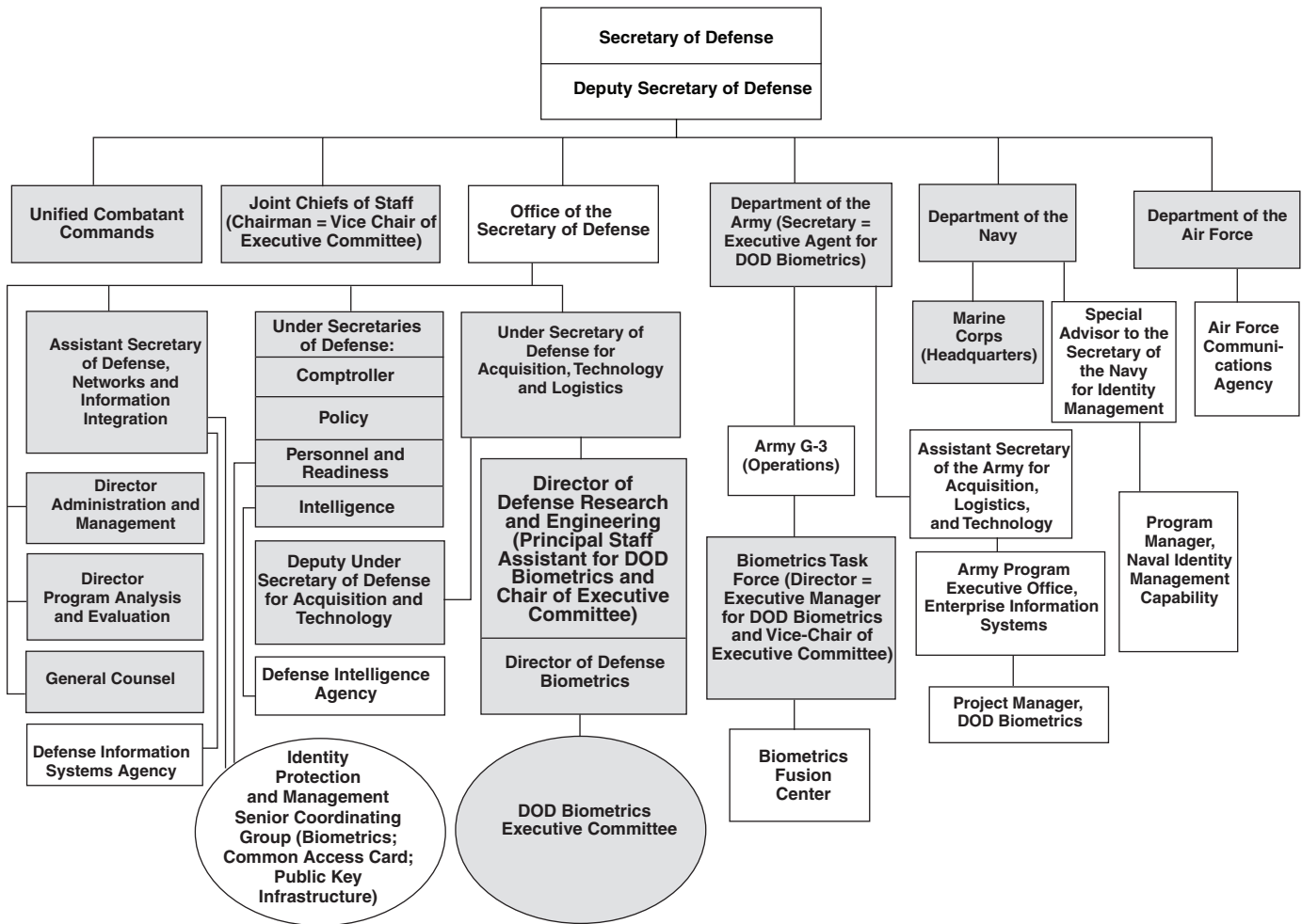
DOD officials said that they have not developed specific strategic goals and objectives and measures of performance characteristic of results-oriented successful programs. According to the Director of Defense Biometrics, who reports to the Principal Staff Assistant, faced with the threat posed by the terrorist attacks of September 11, 2001, DOD has been focusing most of its efforts on quickly fielding biometrics systems, particularly in Iraq and Afghanistan, and working to maximize existing biometrics systems and programs to address DOD's immediate warfighting needs. According to DOD officials, the ongoing Capabilities Based Assessment of the shortfalls in DOD biometrics activities is expected to lay the foundation for the eventual development of a formal biometrics program.¹⁷ The study is expected to be completed in late fall 2008. In addition, the new biometrics directive directed the Executive Manager for Biometrics to develop a new DOD biometrics vision and strategy for submission to the Principal Staff Assistant for Biometrics. According to officials, that document is currently in development and is expected to be completed in late summer 2008.

¹⁷In January 2006, DOD's Director of Defense Research and Engineering issued a memorandum requesting that DOD conduct an in-depth Capabilities Based Assessment of the gaps in the department's overall biometrics capabilities.

**DOD Has Not Established
Implementing Guidance
Clarifying Decision-Making
Procedures for Resolving
Policy and Management
Issues**

Biometrics activities are dispersed throughout DOD at many organizational levels, as shown in figure 2, and DOD has not established implementing guidance clarifying decision-making procedures to minimize duplications of effort and ensure interoperability across these levels. The various offices of the Secretary of Defense, such as those offices associated with intelligence, acquisitions, networks and information integration, personnel, and policy, and the military services each have their own functional or operational requirements and responsibilities for biometrics. However, with many different organizations using biometrics for their own requirements and missions, coordination has been difficult to achieve across DOD.

Figure 2: Key DOD Entities Involved in Biometrics Activities



Source: GAO analysis of DOD documents.

Note: Members of the DOD Biometrics Executive Committee are in shaded boxes.

To address its coordination challenges, DOD established the Executive Committee chaired by the Principal Staff Assistant, with responsibilities that included ensuring the interoperability of DOD’s biometrics systems and resolving important policy or management issues, including disputes that could result in unnecessary duplication of effort. DOD’s establishment of the Principal Staff Assistant and Executive Committee is viewed by many as an improvement over past management approaches. However, the directive establishing the responsibilities of the committee did not

provide guidance to clarify how decisions would be made to resolve disputes over duplication of effort or other important policy or management issues. Our prior work states that in assessing federal programs and best practices of public and private organizations, it is important to clearly identify not only organizational roles and responsibilities but also implementing guidance addressing specific mechanisms and accountability provisions for coordination and collaboration and resolution of conflicts. We have reported that DOD's approach to business operations to support warfighter needs, such as biometrics activities, is a high-risk area that has suffered from pervasive problems in the ability to make coordinated system improvements that cut across multiple organizations.¹⁸ DOD's attempts to make improvements across multiple organizations have often been hindered by fragmented responsibilities for activities and control over resources and in defining accountability and authority for making improvements.

DOD established, in October 2006, the Principal Staff Assistant and the Executive Committee and issued a memorandum that called for the Principal Staff Assistant to have "responsibility for the authority, direction, and control of DOD biometrics programs, initiatives, and technologies" and for developing and coordinating biometrics policy. However, DOD's 2008 directive superseded this memorandum, giving the Executive Committee responsibility for review and approval of DOD biometrics program strategy, program plans, and resources. The directive states that it is DOD policy that biometrics programs shall be designed to improve the effectiveness and efficiency of biometrics activities by "eliminating unwarranted duplication and overlap of technology development and information management efforts." However, the directive allows the military services to acquire biometrics capabilities on their own if such capabilities are determined to be service-specific. The directive requires that the services coordinate with the Executive Committee in this area, and does not specify the mechanism for determining whether biometrics capabilities are service-specific or applicable DOD-wide. As a result, when services pursue their own biometrics systems, these systems may lack interoperability DOD-wide or be duplicative. This has been a problem in the past, as previous DOD studies have noted a serious lack of

¹⁸GAO, *High-Risk Series: An Update*, [GAO-07-310](#) (Washington, D.C.: January 2007).

coordination, interoperability, and ability to share biometric data in Afghanistan and Iraq.¹⁹

DOD officials stated that its acquisition guidelines would provide the needed management discipline over the military services' and components' biometrics activities. However, we have reported repeatedly that significant, systemic problems associated with DOD's acquisition processes at both the strategic and program levels—problems leading to weapon programs that take longer, cost more, and deliver fewer capabilities than originally planned—will require greater discipline and accountability from DOD, as well as other fundamental changes.²⁰ Similarly, as part of DOD's ongoing Capabilities Based Assessment of biometrics in support of identity management at DOD, U.S. Joint Forces Command issued a report in February 2008 noting that without a formal program for biometrics, not all steps associated with safeguards in DOD's acquisitions process for new technological systems are occurring.²¹ According to the report, for example, DOD lacks an approved information architecture for developing and procuring biometrics information systems, defined key performance parameters for designing and procuring biometrics systems, and a defined regime for testing and certifying the interoperability of biometrics systems. Such efforts are key to addressing long-term strategic issues within a broader program for identity management.

¹⁹Biometrics Tiger Team of the Executive Agent for DOD Biometrics, *Biometrics Tiger Team Trip Report 23 April – 5 May 2006*.

²⁰See GAO, *Defense Acquisitions: Better Weapon Program Outcomes Require Discipline, Accountability, and Fundamental Changes in the Acquisition Environment*, [GAO-08-782T](#) (Washington, D.C.: June 3, 2008). The testimony, based on a body of GAO work on DOD's acquisitions processes, states that at the strategic level, DOD's processes for identifying warfighter needs, allocating resources, and developing and procuring weapon systems—which together define DOD's overall weapon system investment strategy—are fragmented and broken. At the program level, the testimony states that weapon system programs are initiated without sufficient knowledge about system requirements, technology, and design maturity.

²¹U.S. Joint Forces Command, *Joint Capabilities Document (JCD): Biometrics in Support of Identity Management* (Norfolk, Va.: Feb. 15, 2008). The report summarizes the results of one phase of the Capabilities Based Assessment led by the command at the request of the Director of Defense Research and Engineering, and identifies capabilities and appropriate tasks that are useful in defining the operational needs for biometrics technology in support of identity assurance—an element of identity management—across the range of military operations.

DOD Has Not Established a Designated Budget to Link Resources and Provide a Consolidated View of Biometrics Resources

DOD has not designated a biometrics budget linking resources to specific objectives and providing a consolidated view of the resources devoted to biometrics activities. Our prior work underscores the importance of taking these actions.²² According to DOD officials, instead of having a designated budget for biometrics as other more established programs have been provided, resources for biometrics activities have been provided primarily through individual, initiative-by-initiative requests for supplemental funding associated with the Global War on Terrorism. Our prior work notes that relying on supplemental funding is not an effective means for decision makers to plan for future years' resource needs, weigh priorities, and assess budget trade-offs.²³

According to DOD officials, the use of supplemental funds creates uncertainty surrounding the implementation of program initiatives, since the use of supplemental funding makes it harder to compete for resources against formally established programs and does not ensure a predictable stream of program funding. For example, in response to U.S. Central Command's August 2005 identification of the urgent operational need to improve biometrics in its operations in Iraq and Afghanistan, DOD developed a series of initiatives to address those needs, with requirements of about \$430 million. Although DOD has made progress in initiatives such as improvements in intelligence and forensics analysis and in fielding additional equipment for the call for an increase in troops, it has reported that many of the initiatives have experienced resource delays and other problems, resulting in systems continuing to experience problems in interoperability—such as inconsistent data formats and screening procedures—that limit DOD's ability to share, screen, and store biometrics data in an efficient, timely manner. According to U.S. Central Command officials, it is difficult to quantify the impact of delays in these initiatives precisely, but time lags in developing these capabilities hinder a commander's ability to engage in population management and reduce the ability to seize and exploit opportunities that may not be present later. Ultimately, such delays can result in catching fewer insurgents and

²²See [GAO-04-408T](#), [GAO-01-159SP](#), and [GAO/GGD-96-118](#).

²³GAO, *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); *Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure*, [GAO-07-461](#) (Washington, D.C.: May 24, 2007); and *Securing, Stabilizing, and Rebuilding Iraq: Key Issues for Congressional Oversight*, [GAO-07-308SP](#) (Washington, D.C.: Jan. 9, 2007).

suboptimal system performance. As of April 2008, about \$275 million of the \$429 million (64 percent) required had been provided for the initiatives.

In conjunction with the previously discussed Capabilities Based Assessment, U.S. Joint Forces Command estimated in August 2007 that about \$2.7 billion—ranging from \$523.4 million to \$558.7 million annually—would be required for a designated budget for DOD biometrics activities from fiscal years 2009 to 2013. These budget estimates included biometrics-related operations and maintenance activities, procurement, and research, development, test, and evaluation for all of the military services, U.S. Northern Command, and U.S. Central Command. According to the Director of Defense Biometrics, these budget estimates were not validated or submitted formally to DOD’s Office of the Comptroller. Officials from this office, however, noted that approval of such a budget would have been uncertain, given DOD’s relatively undeveloped biometrics organizational and management structures and lack of clearly defined long-term biometrics requirements. Instead, according to the Director of Defense Biometrics, the Principal Staff Assistant for DOD Biometrics submitted a request and received approval for \$70 million from fiscal years 2009 to 2013 for the establishment of a U.S. Army biometrics program associated with the Automated Biometric Identification System, DOD’s central repository of biometrics data on non-United States persons of interest. In addition, officials from DOD’s Biometrics Task Force are continuing to develop the information needed for a designated budget that would provide a comprehensive view of DOD’s biometrics activities. Until DOD has established a designated budget, it will continue to experience uncertainty in obtaining resources for its biometrics activities.

In addition to the lack of a designated budget, the Principal Staff Assistant’s authority regarding overall biometrics funding was changed by the 2008 directive on biometrics. Initially, the 2006 memorandum from the Deputy Secretary of Defense that established the Principal Staff Assistant called on the Principal Staff Assistant to “approve biometrics funding across the DOD in support of validated requirements and approved standards and architecture.” However, the 2008 directive changed this role and provides for the Principal Staff Assistant to “review the adequacy of biometrics funding,” while giving the Executive Committee responsibility for reviewing and approving annual program plans and resources for biometrics activities. DOD officials told us that some services and offices opposed the provisions in the 2006 memorandum that gave the Principal Staff Assistant authority to approve funding of all biometrics-related activities because that would have undercut their own funding authorities.

They believed that the potential for “coordinating” their biometrics spending through the Executive Committee provided sufficient opportunity for Principal Staff Assistant review.

Conclusions

Biometrics technologies have become essential tools for supporting DOD’s warfighting and counterterrorism missions, but DOD continues to lack clear goals and performance measures, implementing guidance to specify how the Executive Committee will make decisions to resolve disputes over duplication of effort or other important policy or management issues, and a designated budget—management practices key for program success. While each is important in its own right, these practices also interrelate, with weaknesses in one practice reinforcing and prolonging weaknesses in another. For example, program officials need to establish clear, long-term biometrics goals and objectives to provide program direction. Clear program goals and objectives are needed to justify and prioritize budgetary resources, and in turn, such resources are necessary to accomplish program goals. Similarly, a lack of clear implementing guidance on how decisions to resolve important policy or management issues are made can confuse accountability. Officials say that some of the management weaknesses have occurred because the department’s focus on fielding biometrics systems as quickly as possible to meet immediate, shorter-term warfighting needs has resulted in insufficient attention to developing an overall approach for managing dispersed biometrics activities across the department. However, weaknesses in DOD’s management of its biometrics activities, if allowed to continue, serve to hinder DOD’s ability to effectively support its warfighting and counterterrorism missions in the long term. For example, continuing interoperability problems among several major biometrics systems in U.S. Central Command’s area of operations—problems involving inconsistent biometrics data formats and screening procedures—have impeded the command’s ability to share biometrics data in an efficient, timely manner. Furthermore, according to U.S. Central Command officials, several high-priority departmental initiatives intended to address such problems—identified as “urgent operational needs” in 2005 by the command—were delayed, thereby jeopardizing the command’s ability to identify and detain potential enemy combatants. In addition, shortcomings in DOD’s management of biometrics activities may impede the department’s efforts to fully implement the June 2008 presidential directive on using biometrics within the federal government to enhance national security, as well as hinder DOD’s ability to further develop the overall identity management operating concept. As a result, we believe that the department needs to

take a longer-term perspective on the management of its biometrics initiatives.

Recommendations for Executive Action

To improve the management of DOD's biometrics activities, we recommend that the Secretary of Defense direct the Principal Staff Assistant and Executive Committee to (1) develop clearly defined goals and measures of success to guide and monitor development of biometrics activities, (2) issue implementing guidance that clarifies decision-making procedures for the Executive Committee, and (3) work with the Comptroller to establish a designated biometrics budget.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD concurred with all of our recommendations. Also, the Director of Defense Biometrics provided us with technical comments, which we incorporated in the report where appropriate. DOD's written comments are reprinted in appendix V.

DOD concurred with our first recommendation that the Secretary of Defense direct the Principal Staff Assistant and the Executive Committee for DOD Biometrics to develop clearly defined goals and measures of success to guide and monitor the development of DOD's biometrics activities. In its concurrence with this recommendation, DOD indicated that the Executive Committee had approved a *DOD Biometrics Enterprise Strategic Plan (2008-2013)* while the department was reviewing a draft of this report. According to DOD, the strategy includes specific goals and objectives for DOD's biometrics enterprise and directs the development of a detailed implementation plan that includes metrics and milestones. DOD further stated that it would develop additional milestones and metrics for emerging biometrics acquisitions programs in conjunction with the development of a more formal biometrics program. We did not have an opportunity to review the DOD Biometrics Enterprise Strategic Plan before publishing this report and therefore did not evaluate the extent to which the plan's goals and measures of success would help guide and monitor the development of DOD's biometrics activities.

DOD also concurred with our second recommendation that the Secretary of Defense direct the Principal Staff Assistant and the Executive Committee for DOD Biometrics to issue implementing guidance that clarifies decision-making procedures for the Executive Committee. In its concurrence with this recommendation, DOD noted that the Executive Committee had initiated the development of an implementation instruction to clarify and provide details about the governing process for

DOD biometrics. The department expects approval of this guidance in fiscal year 2009.

Finally, DOD concurred with our third recommendation that the Secretary of Defense direct the Principal Staff Assistant and the Executive Committee for DOD Biometrics to work with the department's Comptroller to establish a designated biometrics budget. In its concurrence, DOD agreed with the need for defined biometrics programs and associated funding lines. The department stated that it had established a discrete biometrics science and technology program in fiscal year 2008 in order to focus biometrics technology development within a primary program. In addition, DOD stated that it had taken significant steps, such as its ongoing Capabilities Based Assessment of biometrics, to transition its biometrics acquisition efforts into more structured programs with associated funding lines. The department intends to initiate such biometrics programs in fiscal year 2010. However, noting that biometrics is an enabling technology that supports many departmental capabilities, DOD intends to establish multiple discrete programs with associated funding lines, rather than a single funding line that encompasses all DOD investments in biometrics technology, systems, and programs. In our view, however, pursuing an approach involving multiple funding lines, DOD should ensure that the funding lines are clearly linked to specific biometrics program objectives and that they provide a consolidated view of the resources devoted to biometrics activities throughout the department.

We are sending copies of this report to the Secretary of Defense and to interested congressional committees. Copies of this report will also be made available to others upon request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you 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. Key contributors to this report are included in appendix VI.

A handwritten signature in black ink, reading "Davi M. D'Agostino". The signature is stylized with large, flowing loops and a cursive script.

Davi M. D'Agostino
Director, Defense Capabilities
and Management

Appendix I: Scope and Methodology

In this report, we examine the extent to which the Department of Defense (DOD) has established biometrics goals and objectives, implementing guidance for managing biometrics activities, and a designated budget to provide a consolidated view of resources devoted to DOD biometrics activities. To address this objective, we considered leading management practices and principles related to these areas and previously identified in prior GAO reports and analyses.¹ Our analysis focused primarily on DOD's management of biometrics activities, systems, and programs associated with its current warfighting and counterterrorism efforts, particularly those used in U.S. Central Command's geographic area of responsibility, which includes Iraq and Afghanistan.

In assessing DOD's efforts, we reviewed documents and interviewed officials from a range of DOD organizations involved in conducting, managing, or overseeing biometrics activities and funding. Specifically, we obtained information from DOD officials representing the Office of the Secretary of Defense (the Under Secretaries of Defense for Acquisition, Technology and Logistics and Intelligence, Policy, Personnel and Readiness; the Comptroller/Chief Financial Officer; the Assistant Secretary of Defense for Networks and Information Integration; and the Director of Administration and Management); the military departments and services (the U.S. Army, the U.S. Navy, the U.S. Air Force, and the Marine Corps); U.S. Joint Forces Command; U.S. Central Command; U.S. Special Operations Command; the Director of Defense Research and Engineering (DOD's Principal Staff Assistant for DOD Biometrics); the Director of Defense Biometrics; the U.S. Army (whose Secretary serves as DOD's Executive Agent for DOD Biometrics); the DOD Biometrics Executive Committee; DOD's Identity Protection and Management Senior Coordinating Group; DOD's Biometrics Task Force; DOD's Program Manager for Biometrics; the Biometrics Fusion Center; the Defense Manpower Data Center (regarding DOD's Common Access Card); DOD's Public Key Infrastructure Program Management Office; and the National Ground Intelligence Center. The documents we reviewed included memorandums, directives, guidance, briefings, progress reports, budgetary data, planning documents, charters, agendas, reports, studies, and analyses related to biometrics activities in the department.

To understand DOD's biometrics activities within a federal government context, including identity management, we also obtained documents and interviewed officials from other federal agencies and offices, such as the Department of Homeland Security, the Department of State, the Federal

¹See [GAO-04-408T](#), [GAO-01-159SP](#), and [GAO/GGD-96-118](#).

Bureau of Investigation, the Office of the Director of National Intelligence, and the National Science and Technology Council's Subcommittee on Biometrics and Identity Management. We also reviewed the June 2008 national security presidential directive on the use of biometrics to enhance national security.²

We conducted this performance audit from May 2007 through September 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.

²The White House, National Security Presidential Directive/NSPD-59, and Homeland Security Presidential Directive/HSPD- 24, *Biometrics for Identification and Screening to Enhance National Security*.

Appendix II: DOD Actions to Improve Coordination of Biometrics

DOD took the following actions from fiscal year 2000 through fiscal year 2008.

In July 2000, Congress designated the Secretary of the Army as the Executive Agent to lead, consolidate, and coordinate all biometrics information assurance programs across DOD.¹

To assist the Executive Agent, DOD created, in December 2000, the Biometrics Management Office—currently known as the Biometrics Task Force—within the Army to consolidate oversight and management for all biometrics technologies for DOD. In August 2002, the Department of the Army also added another organization to coordinate its biometrics activities by establishing the DOD Biometrics Senior Coordinating Group. The group was intended to provide strategic guidance and to serve as a DOD-wide coordinating group for biometrics. Members of the group included various Office of the Secretary of Defense offices, DOD agencies, and the military services.

In January 2004, however, DOD acknowledged the need to improve coordination of its biometrics programs with two other closely linked technology-based initiatives called the Common Access Card and Public Key Infrastructure² programs. To address this need, DOD established the Identity Management Senior Coordinating Group. This organization was to be a “cohesive DOD-wide policy, requirements, strategy, and oversight group” for managing biometrics and the other two initiatives and replaced the existing oversight and coordination bodies for these initiatives (including the Biometrics Senior Coordinating Group). In establishing this new coordinating group, the Assistant Secretary of Defense for Networks and Information Integration acknowledged that the lack of an overarching management vision had impeded development of DOD-wide requirements for a biometrics program.

In response to the continuing problems in biometrics, the Deputy Secretary of Defense established the position of Principal Staff Assistant for DOD Biometrics in the Office of the Under Secretary of Defense for

¹Pub. L. No. 106-246, § 112 (2000).

²Public Key Infrastructure is a system of hardware, software, policies, and people that when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, and authentication—important in protecting sensitive communications.

Acquisition, Technology and Logistics on October 4, 2006. The memorandum establishing the Principal Staff Assistant laid out a strong role for the office, providing it “with responsibility for the authority, direction, and control of DOD biometrics programs, initiatives, and technologies.” The memorandum called for the Principal Staff Assistant to “develop and coordinate DOD biometrics policy” and to “approve biometrics funding across the DOD in support of validated requirements and approved standards and architecture.” The memorandum also called for development of a DOD biometrics directive and the establishment of the Executive Committee for DOD Biometrics to support the Principal Staff Assistant and help ensure “timely and vigorous action.” The memorandum continued the Secretary of the Army’s designation as Executive Agent for DOD’s biometrics programs.

DOD finalized DOD Directive 8521.01E on DOD Biometrics in February 2008, which superseded the 2006 memorandum. The directive laid out general organizational responsibilities for biometrics and established broad DOD policy, such as the need to fully integrate biometrics into DOD operations, eliminate unwarranted duplication and overlap of efforts, and ensure that biometrics capabilities are developed to be interoperable with other identity management capabilities and systems. One of the initial acts of the Principal Staff Assistant was to call for a comprehensive assessment of the shortfalls in departmentwide biometrics activities and the needed solutions. That study, the Capabilities Based Assessment of biometrics in support of identity management, was originally scheduled to be completed by August 2007. However, the assessment continues and is expected to be completed in late fall 2008. According to DOD officials, the rapid development of biometrics capabilities simply outran the policy framework needed to support it.

Appendix III: GAO Management Letter to the Secretary of Defense



G A O

Accountability • Integrity • Reliability

United States Government Accountability Office
Washington, DC 20548

December 13, 2007

The Honorable Robert M. Gates
The Secretary of Defense

Dear Mr. Secretary:

As you know, we are currently reviewing the Department of Defense's (DOD's) use of biometrics to improve identity management. This work is being done at the request of the Chairmen and Ranking Members of the House Armed Services Committee's Subcommittees on Readiness and on Terrorism and Unconventional Threats and Capabilities (engagement code 351028). Specifically, the Subcommittees asked us to review DOD's approach to planning and implementing its biometrics and identity management activities, as well as DOD's efforts to coordinate such activities within the Department and with other federal agencies. We expect to issue a comprehensive report on these issues in the fall of 2008.

During the course of our review, we evaluated DOD's ongoing efforts to develop a DOD directive for Defense biometrics, as called for by the Deputy Secretary of Defense's memorandum on Defense Biometrics dated October 4, 2006. The memorandum called for significant changes to DOD's framework for coordinating its biometrics and identity management activities, including the designation of a Principal Staff Assistant (PSA) with responsibility for the authority, direction, and control over DOD's biometrics activities.

The purpose of this letter is to request that you clarify the intended scope of authority for the PSA, and to urge you to ensure that the final directive provides the PSA with sufficient authority to improve the coordination and direction of DOD's biometrics initiatives. Based on our analysis of the memorandum and the two draft versions of the directive (Number 8521.aaE), we are concerned that the current version of the draft directive would not provide the new PSA for Biometrics with clear authority to direct and oversee DOD's widely dispersed biometrics initiatives as called for in the Deputy Secretary's memorandum.

Such clear authority for the PSA is important to enable DOD to address past problems in its coordination and oversight of biometrics initiatives. DOD has struggled for years to develop a coordinated, cohesive approach to managing the many biometrics initiatives dispersed throughout the Department. These efforts date back at least to July 2000, when the Congress passed Public Law 106-246 directing DOD to designate the Army as the "Executive Agent" to lead, consolidate, and

coordinate all biometrics programs across DOD. Shortly after, the Secretary of Defense created the Biometrics Management Office (BMO)—now known as the Biometrics Task Force—within the Army, to consolidate oversight and management for all biometrics technologies for DOD, and the Biometrics Fusion Center to test, evaluate, and integrate such technologies. Some twenty months later, in August 2002, the Department of the Army added another coordinating organization, announcing that it was establishing a DOD Biometrics Senior Coordinating Group to provide strategic guidance to the BMO and to serve as a DOD-wide coordinating group for biometrics.

Again in January 2004, DOD acknowledged the need to improve coordination of the biometrics programs and two other closely linked initiatives called the Common Access Card and Public Key Infrastructure programs. To address this need, the Assistant Secretary of Defense for Networks and Information Integration established an Identity Management Senior Coordinating Group (IMSCG) to manage and oversee the three initiatives as one coordinated venture across DOD. The Group was to be a “cohesive DOD-wide policy, requirements, strategy, and oversight group” for managing biometrics and the other two initiatives. Shortly thereafter in February 2004, the Assistant Secretary also acknowledged that the lack of an overarching identity management vision had impeded development of DOD-wide requirements for a biometrics program, as well as the Public Key Infrastructure and Common Access Card programs, and directed the IMSCG to formulate a DOD-wide corporate vision for identity management, including biometrics initiatives.

Despite these efforts, DOD organizations have continued to report problems in DOD’s coordination and management of biometrics activities. For example, in an August 2005 *Joint Urgent Operational Need Statement for a Joint Biometrics Solution in Support of Operations*, the U.S. Central Command reported on the “lack of a comprehensive management approach to the development and implementation of biometrics technology,” with DOD services and agencies fielding multiple biometrics systems at varying levels of interoperability. In its review of biometrics systems and processes used in the U.S. Central Command’s area of responsibility, a “Biometrics Tiger Team” reported numerous instances of questions about biometrics leadership in June 2006.

Similarly, in April 2006, the Under Secretary of Defense requested that the Defense Science Board (DSB) form a Task Force to study the Defense Biometrics Program, citing the “reactive” and “ad hoc” nature of DOD’s management of biometrics initiatives since the terrorist attacks of September 11, 2001. The Task Force provided DOD with an interim briefing on the immediate organizational needs—including the need for a Principal Staff Assistant for Biometrics—in May 2006, and its final report in March 2007. In its final report, the Task Force reported that the “Operational responsiveness, organization, coordination, [and] programmatic [of DOD’s biometrics activities]...all showed serious deficiencies...” Among its various recommendations, the Task Force called for DOD to clarify, strengthen, and reassign roles, responsibilities, and authorities of DOD components involved in managing biometrics initiatives.

In response to concerns such as those cited in the DSB report, the Deputy Secretary of Defense issued a memorandum on Defense Biometrics on October 4, 2006. Among its key provisions, the memorandum designated the Director of Defense Research and Engineering (DDR&E), under the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), as DOD's Principal Staff Assistant (PSA) for Biometrics "with responsibility for the authority, direction, and control of DOD biometrics programs, initiatives, and technologies." The memorandum called for the PSA, with the assistance of a newly established Director for Defense Biometrics, to "develop and coordinate DOD biometrics policy" through the USD(AT&L) and to "approve biometrics funding across the DOD in support of validated requirements and approved standards and architecture."

The memorandum also called for the establishment of an Executive Committee for Biometrics to support the PSA with high-level representatives from the Department's policy, operations, intelligence, personnel, acquisition, and information communities, as well as the military departments. In addition, the memorandum continued the Secretary of the Army's designation as Executive Agent for DOD's biometrics programs, with responsibility for ensuring that biometric data are fully accessible to required users and for supporting the implementation of joint biometrics capabilities, including joint standards, architecture, and research and development activities.

Finally, the memorandum called for DDR&E to lead the development of a DOD directive implementing the provisions of the memorandum and delineating the roles and responsibilities of relevant DOD stakeholders. In July 2007, DDR&E submitted an initial draft of this directive – DOD Directive 8521.aaE on "the DOD Biometrics Program" – to relevant DOD offices and military services for formal coordination, review, and comment. Although the comments received from these stakeholders covered a range of issues, several of them – including some categorized as "critical" nonconcurrence – reflected concerns over the extent of the PSA's oversight authorities. In order to address these comments and concerns and obtain full concurrence from the DOD stakeholders, DDR&E subsequently drafted a revised version of the directive in September 2007.

Based on our review of the draft versions of the directive, we are concerned that certain provisions in the latest version do not appear fully consistent with the Deputy Secretary of Defense's memorandum of October 4, 2006. In particular, provisions in the current draft would provide the PSA with considerably less authority to oversee and coordinate DOD's biometrics initiatives than originally called for in the memorandum. As previously mentioned, such authority for the PSA is important if DOD is to develop a coordinated, cohesive approach to managing its various biometric initiatives.

The memorandum, for example, called for the PSA to approve biometrics funding across DOD, including the spending plans of DOD components for executing their biometrics programs. However, the current draft of the Directive indicates that the DDR&E would only "review the adequacy of biometrics funding across the DOD..." The memorandum also called for the PSA to coordinate DOD biometrics policy department-wide. In three instances, however, provisions in the current draft of the Directive were either added or modified from those in the initial draft to require only that DOD offices would coordinate their biometrics-related programs and budget

through their participation in the Executive Committee for Biometrics, rather than directly with the PSA. Similarly, in three instances, provisions in the initial draft of the Directive that called for DOD offices to support or coordinate directly with the PSA on certain issues were deleted from the current draft.

According to DOD officials, these changes reflect concerns expressed by some military services and DOD offices involved in the development of the Directive over the extent of the PSA's responsibilities and authorities. For example, officials told us that some services and offices opposed the provisions giving the PSA authority to approve funding of all biometrics-related activities, because that would have conflicted with their own funding authorities, already established under Title 10 of the U.S. Code. They believed that the potential for coordinating their biometrics spending through the Executive Committee provided sufficient opportunity for PSA review. However, this approach provides no formal mechanism for review and approval and does not prevent DOD organizations from spending on biometrics activities in ways that may not be consistent with DOD-wide views of the PSA. Officials told us that in the case of disagreements, the PSA would be free to raise his concerns to the DOD Comptroller, Deputy Secretary, or Secretary of Defense. Some officials also indicated that the Executive Committee should play a greater role than the PSA or EA in providing strategic guidance and direction, since its decisions reflect consensus from high-level representatives of all relevant DOD services and offices. One official stated that it would be inappropriate for the EA, acting on behalf of the PSA, to provide direction to other offices operating at the secretarial level, when the EA itself was not a secretarial level organization in the Department of the Army.

Although we appreciate such concerns and recognize that the directive would represent an important step in improving DOD's management of its biometrics activities, we note that the Deputy Secretary of Defense's memorandum clearly intended for the PSA to have "responsibility for the authority, direction, and control of DOD biometrics programs, initiatives, and technologies" and to "approve biometrics funding across the DOD..." The lack of integration, discipline and leadership have consistently been identified as problems hampering progress in the biometrics program. We are concerned that if the PSA does not have the requisite authority needed to resolve potential conflicts of interest among DOD services and offices over the strategic direction or funding of biometrics initiatives, DOD will again be in the same position. Furthermore, resolving such conflicts through the DOD Comptroller, the Deputy Secretary of Defense, or the Secretary of Defense – as proposed by some DOD services and offices – would appear to contradict the leadership role for the PSA envisioned in the Deputy Secretary of Defense's memorandum.

In light of these differences, we request that you clarify DOD's intended scope of oversight authority for the PSA and urge you to ensure that DOD's final directive provides the PSA with sufficient authority to improve the coordination and direction of DOD's biometrics initiatives. This is particularly important as DOD seeks to integrate its biometrics initiatives within the broader framework of identity

management and identity superiority in the future. Please direct your response, and any questions you or your staff may have, to me at (202) 512-5431 or DAgostinoD@gao.gov, or to David Artadi of my staff at (404) 679-1989 or ArtadiD@gao.gov. We are sending copies of this letter to the House Armed Services Committee, Subcommittees on Readiness and Terrorism, Unconventional Threats and Capabilities.

Sincerely yours,



Davi M. D'Agostino, Director
Defense Capabilities and Management

(351126)

Page 5

Appendix IV: DOD Response to GAO Management Letter



ACQUISITION,
TECHNOLOGY
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

FEB 13 2008

Mr. Davi M. D'Agostino
Director, Defense Capabilities and Management
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. D'Agostino:

Thank you for your letter to the Secretary of Defense concerning the authorities assigned to the Principal Staff Assistant for DoD Biometrics. Your letter correctly highlights the need to have clear authorities assigned to ensure effective development and coordination of DoD biometrics capabilities. The policy and governance structure that is outlined in the draft DoD Directive 8521.aaE provides the Director, Defense Research and Engineering (DDR&E), my principal staff assistant (PSA) for Defense Biometrics, with clear responsibilities and strong authority to achieve an effective and enduring biometrics capability to support Department requirements.

Prior to assignment of the PSA, there were deficiencies in the coordination and oversight of the efforts being independently undertaken by the various DoD components dating back to July 2000. In view of the expanding operational value of biometrics, DDR&E was assigned as the PSA with authority to control, direct and, ultimately, mature the DoD biometrics programs. Although not specifically stated in the October 2006 Deputy Secretary of Defense memorandum, a critical implied responsibility of the PSA was to transition the various ad hoc biometrics efforts into the Department's mainstream acquisition process with its inherent and strict oversight authorities.

The directive as drafted does not diminish the PSA authority; it establishes structures and processes through which to exercise that authority in an efficient and transparent manner consistent with DoD Joint Capability Development and acquisition guidelines. Although the language of the memorandum and the draft directive are different, the authorities of the PSA have not been diminished. The PSA continues to execute approval authority over component programs and resources, but that authority will be executed through the biometrics Executive Committee (EXCOM), chaired by the PSA, thereby ensuring transparency and full coordination of the Department's biometrics programs.

Additionally, the draft directive makes all components responsible and accountable to the PSA for reviewing all biometrics requirements and programs and



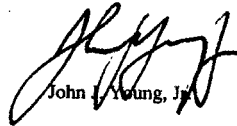
submitting such to the EXCOM for review and approval. To provide the requisite programmatic discipline for this enduring capability, the directive further requires full compliance with DoD acquisition guidelines and directs the Army as the Executive Agent to appoint a Program Manager accountable through the Army Acquisition Executive. To further ensure component compliance, the directive further requires the PSA to submit an annual report to the Secretary of Defense on the adequacy of the program's assignments, arrangements, and funding. All of these controls serve to strengthen the oversight of our biometrics programs and provide the PSA with the tools he needs to hold all components accountable for compliance.

The desired outcome of our biometrics directive is an effective management structure, consistent with Department and regulatory acquisition guidance. The Secretary of the Army has clear responsibility and authority as Executive Agent for managing common Department-wide biometrics functions while requiring the many DoD components to fully coordinate their activities and gain approval prior to program initiation or procurement actions.

Under DDR&E's leadership this past year, we have begun to normalize the acquisition and operation of biometrics technologies within the Department resulting in much improved performance and maintainability of our systems. We are conducting a full Capability-Based Assessment to enhance development, and the Services are planning for these capabilities in their programs and developing their own internal management structures. The roles and responsibilities assigned to the DoD components, with oversight provided by the PSA as outlined in the draft directive, is not only adequate, but provides the best path for stabilizing the management of this important technical capability as its value to DoD expands.

My point of contact is Mr. Tom Dee, Director Defense Biometrics, at 703-746-1385.

Sincerely,



John L. Young, Jr.

Appendix V: Comments from the Department of Defense



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

SEP 12 2008

Mrs. Davi M. D'Agostino
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mrs. D'Agostino:

This is the Department of Defense (DoD) response to the GAO draft report, GAO-08-1065, "DEFENSE MANAGEMENT: DoD Needs to Establish Clear Goals and Objectives, Guidance, and a Designated Budget to Manage Its Biometrics Activities," dated August 13, 2008 (GAO Code 351028).

The Department concurs with the need for continued improvement of the management processes which govern the Department's biometrics programs. The establishment of clear program goals and objectives and the issuance of implementing guidance for DOD Directive 8521.01E (Defense Biometrics) were identified as priorities by the Department's Biometrics Executive Committee and the establishment of programmed funding for the biometrics programs is the subject of an ongoing review by the Department.

The Department also agrees with GAO's comments concerning the interrelationship of the three recommendations. Designated program funding requires clear program requirements, objectives and milestones. These objectives and milestones, however, cannot be attained without adequate program funding. To accurately assess the scope of our biometrics programs and to enable the initiation of formal biometrics programs of record, the Department initiated a capabilities based assessment that will be concluded shortly. This assessment will objectively identify priority capability gaps, recommend solutions to overcome those gaps and inform our decision as to how to best structure our acquisition efforts and the associated funding.

Sincerely,

A handwritten signature in black ink, appearing to read "Alan R. Shaffer".

Alan R. Shaffer
Principal Deputy

Enclosure:
As stated



GAO Draft Report Dated August 13, 2008
GAO-08-1065 (GAO CODE 351028)

**“DEFENSE MANAGEMENT: DoD Needs To Establish Clear Goals and
Objectives, Guidance and a Designated Budget To Manage Its
Biometrics Activities”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS**

RECOMMENDATION 1: That the Secretary of Defense direct the Principal Staff Assistant and the Executive Committee to develop clearly defined goals and measures of success to guide and monitor development of biometrics activities.

DOD RESPONSE: Concur. The establishment of clear program goals and objectives and the associated metrics and milestones was identified as a priority by the Department’s Biometrics Executive Committee which approved the DoD Biometrics Enterprise Strategic Plan (2008-2013) at its 27 Aug 2008 quarterly meeting. This strategy includes specific goals and objectives for our biometrics enterprise and directs the development of a detailed implementation plan, currently in progress, which includes metrics and milestones. Milestones and metrics for emerging biometrics acquisition programs will be developed and approved coincident to the development of biometrics programs of record and consistent with defense acquisition guidelines.

RECOMMENDATION 2: That the Secretary of Defense direct the Principal Staff Assistant and the Executive Committee to issue implementing guidance that clarifies decision-making procedures for the Executive Committee.

DOD RESPONSE: Concur. The Department’s Executive Committee initiated the development of an implementation instruction to clarify and detail the governing process for the Department’s biometrics enterprise. Approval of this guidance is expected in FY 2009.

RECOMMENDATION 3: That the Secretary of Defense direct the Principal Staff Assistant and the Executive Committee to work with the Comptroller to establish a designated biometrics budget.

DOD RESPONSE: Concur. The Department concurs with the need for defined biometrics programs and associated funding lines in order to provide the structure to succeed within our acquisition processes and the predictability upon which to build and gauge our capabilities. To that end, the Department established a discrete biometrics Science and Technology program in FY08 in order to better focus biometrics technology development within a primary program. Similarly, we have taken significant steps to transition our biometrics acquisition efforts into formal programs of record with associated funding lines. We will shortly complete a Biometrics Capabilities Based Assessment that defines our priority capability gaps and proposes both material and non-material solutions. The Army and Navy both initiated follow-on Capability

**Appendix V: Comments from the Department
of Defense**

Development Documents which will form the basis of our biometrics programs of record. We are currently assessing the scope of these programs and the requisite level of resources to support them. We intend to have both the programs and funding in place to enable formal program initiation in FY10. As biometrics is an enabling technology that supports many department capabilities, however, we do not anticipate having a single funding line that encompasses all department investment in biometric technology, systems and programs. Rather the intent is to establish discrete programs with associated funding lines that best captures the program scope and purpose while providing Department level visibility of our collective biometrics efforts.

Appendix VI: 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, Linda Kohn, Acting Director; Lorelei St. James, Assistant Director; David Artadi; Grace Coleman; Brian Kime; David Malkin; John Nelson (retired); and Bethann Ritter made key contributions to this report.

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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

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