



ENGINEERING-PDH.com
ONLINE CONTINUING EDUCATION

DEPLOYABLE DOD BIOMETRIC FORENSICS

Main Category:	Electrical Engineering
Sub Category:	-
Course #:	ELE-143
Course Content:	55 pgs
PDH/CE Hours:	4

OFFICIAL COURSE/EXAM

(SEE INSTRUCTIONS ON NEXT PAGE)

WWW.ENGINEERING-PDH.COM

TOLL FREE (US & CA): 1-833-ENGR-PDH (1-833-364-7734)

SUPPORT@ENGINEERING-PDH.COM

ELE-143 EXAM PREVIEW

- TAKE EXAM! -

Instructions:

- At your convenience and own pace, review the course material below. When ready, click “Take Exam!” above to complete the live graded exam. (Note it may take a few seconds for the link to pull up the exam.) You will be able to re-take the exam as many times as needed to pass.
- Upon a satisfactory completion of the course exam, which is a score of 70% or better, you will be provided with your course completion certificate. Be sure to download and print your certificates to keep for your records.

Exam Preview:

1. In 2014 the Secretary of the Army designated the Defense Forensics and Biometrics Agency (DFBA) as the executive manager and tasked the agency with carrying out the Army’s biometric and forensic executive agent responsibilities
 - a. True
 - b. False
2. According to the reference material, A goal of the rapid acquisition process is to typically field a capability solution to an urgent or emergent operational need within ___ years.
 - a. 2
 - b. 3
 - c. 4
 - d. 5
3. The DoD has several biometric collection capabilities. Which of the following choices below corresponds to: SOCOM hand-held device attached to a cellular phone used to collect fingerprint, iris, facial images, and biographical information?
 - a. Secure Electronic Enrollment kit
 - b. Biometrics Automated Toolset
 - c. Identity Dominance System
 - d. BioSled
4. In fiscal year 2016 DOD ABIS’s average match/no-match response time was generally between 1 and 11 minutes, depending on the prioritization level assigned to the biometric submission.
 - a. True
 - b. False

5. The DoD has several forensic analysis capabilities. Which of the following choices below corresponds to: Managed by the Navy, this tool is a laboratory-information management and database sharing software system for documenting, tracking, reporting, and sharing forensic data?
 - a. Exploitation Analysis center
 - b. Expeditionary Forensic Exploitation Capability
 - c. Forensic Exploitation Analysis Tool
 - d. Forensic Exploitation Laboratories
6. According to DOD guidance, no later than 1 year after a system enters operation and sustainment, DOD should complete a disposition analysis that recommends a course of action, including whether to retain the system.
 - a. True
 - b. False
7. Using Figure 4 of the reference material, which of the following geographic commands includes the US and Canada?
 - a. EUCOM
 - b. NORTHCOM
 - c. CENTCOM
 - d. SOUTHCOM
8. Table 1 lists the non-materiel Enduring Requirements for Deployable Biometric and Forensic Capabilities by Area. Using this table, how many validated requirements does Training need?
 - a. 2
 - b. 3
 - c. 6
 - d. 9
9. According to Figure 4 of the reference material, the U.S. Pacific Command (PACOM) includes major countries such as Australia, China, Japan, and Russia
 - a. True
 - b. False
10. Table 2 lists the non-materiel Biometric and Forensic Requirements Reflecting Significant Progress as Assessed by the Defense Forensics and Biometrics Agency. Using this chart, what is the reported completion status on Forensics Policy?
 - a. 100 %
 - b. 90 %
 - c. 75 %
 - d. 50 %

Contents

Letter	1
Background	4
DOD Has Validated Enduring Requirements for Deployable Biometric and Forensic Capabilities	12
DOD Has Taken Actions to Meet Enduring Biometric and Forensic Requirements but Faces Challenges in Sustaining Progress	15
DOD Has Implemented Almost All of Our Prior Biometric- and Forensic-related Recommendations	25
Conclusions	27
Recommendations for Executive Action	28
Agency Comments and Our Evaluation	29
Appendix I: Objectives, Scope, and Methodology	30
Appendix II: Geographic Combatant Commands' Demand for Biometric and Forensic Capabilities	35
Appendix III: Department of Defense (DOD)-Validated, Non-materiel Enduring Biometric and Forensic Requirements	37
Appendix IV: Additional Actions Taken by Department of Defense (DOD) on Previously Closed GAO Recommendations	40
Appendix V: Comments from the Department of Defense	44
Appendix VI: GAO Contact and Staff Acknowledgments	47
Appendix VII: Accessible Data	48
Agency Comment Letter	48
Related GAO Products	52

Tables

Table 1: Department of Defense (DOD)-Validated, Non-materiel Enduring Requirements for Deployable Biometric and Forensic Capabilities, by Area	14
Table 2: Non-materiel Biometric and Forensic Requirements Reflecting Significant Progress as Assessed by the Defense Forensics and Biometrics Agency, by Area ^a	16
Table 3: Status of the Department of Defense's (DOD) Implementation of Our Biometric and Forensic Recommendations since 2011, as of May 2017	25
Table 4: Department of Defense (DOD) Organizations Contacted by GAO ^a	32
Table 5: Biometric and Forensic Non-materiel Enduring Requirement Status ^a	37
Table 6: Additional Department of Defense (DOD) Actions Taken on Previously Closed Biometric and Forensic Recommendations	40

Figures

Figure 1: Biometric Automated Toolset and Secure Electronic Enrollment Kit Collection Devices in Use	7
Figure 2: Examples of Forensic Exploitation Laboratory Modules	9
Figure 3: Example of Biometrics Used to Identify a Person of Interest	11
Figure 4: Geographic Combatant Commands' Demand for Biometric and Forensic Capabilities	13

GAO Highlights

Highlights of [GAO-17-580](#), a report to congressional committees

Why GAO Did This Study

Since 2008 DOD has used biometric and forensic capabilities to capture or kill 1,700 individuals and deny 92,000 individuals access to military bases. These capabilities were mainly developed through rapid acquisition processes and were resourced with Overseas Contingency Operations funds—funds that are provided outside of DOD's base budget process. As a result, concerns have been raised about DOD's long-term ability to fund these capabilities.

The House Armed Services Committee and House Permanent Select Committee on Intelligence included provisions in committee reports for GAO to review DOD's progress in institutionalizing deployable biometric and forensic capabilities. This report examines, among other issues, the extent to which DOD since 2011 has (1) validated long-term requirements for deployable biometric and forensic capabilities; and (2) taken actions to meet long-term requirements for deployable biometric and forensic capabilities and overcome any related challenges. GAO examined DOD directives, strategies, policies, plans, and requirements and met with cognizant DOD officials.

What GAO Recommends

GAO is making 6 recommendations, including that DOD update its biometric enterprise strategic plan; take steps to more effectively manage the acquisition of a recent biometric capability; and consider developing a geographically dispersed back-up capability for its authoritative biometric database. DOD concurred with all of the recommendations and cited actions it plans to take to address them.

View [GAO-17-580](#). For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or KirschbaumJ@gao.gov.

August 2017

DOD BIOMETRICS AND FORENSICS

Progress Made in Establishing Long-term Deployable Capabilities, but Further Actions Are Needed

What GAO Found

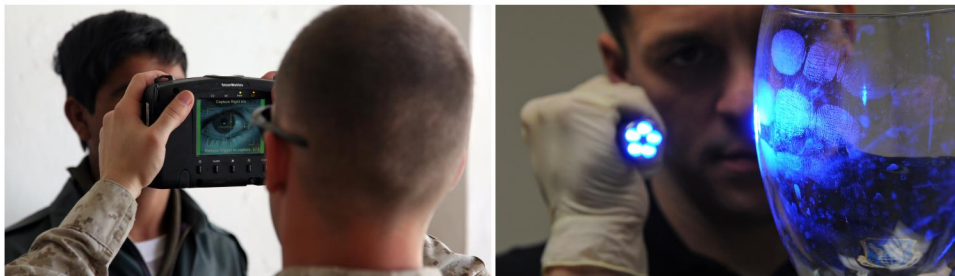
The Department of Defense (DOD) has validated its requirements for long-term deployable biometric capabilities (such as fingerprint collection devices) and forensic capabilities (such as expeditionary laboratories). Biometric capabilities are used to identify individuals based on measurable anatomical, physiological, and behavioral characteristics such as fingerprints, iris scans, and voice recognition. Forensic capabilities support the scientific analysis of evidence—such as deoxyribonucleic acid (DNA) and latent fingerprints—to link persons, places, things, and events. DOD utilizes deployable biometric and forensic capabilities to support a range of military operations, such as targeting, force protection, and humanitarian assistance.

DOD has made significant progress in addressing its long-term requirements for deployable biometric and forensic capabilities, such as issuing new doctrine and establishing long-term funding for several capabilities, including DOD's authoritative biometric database that is used for identifying enemy combatants and terrorists. However, DOD's efforts to institutionalize these capabilities are limited by the following strategic planning gaps and acquisition management challenges:

- While DOD has a current and approved forensic strategic plan, it does not have one for its biometric capabilities, because no entity has been assigned responsibility for developing such a plan, according to DOD officials.
- The Army did not follow DOD's acquisition protocols in developing a recent key biometric capability, and it may have missed an opportunity to leverage existing, viable, and less costly alternatives.
- DOD's authoritative biometric database that is used for identifying enemy combatants and terrorists does not have a geographically dispersed back-up capability to protect against threats such as natural hazards. Having such a back-up could enhance the database's availability.

Addressing these strategic planning and acquisition management challenges could help DOD sustain the progress it has made to establish enduring deployable biometric and forensic capabilities.

U.S. Military Personnel Apply Biometric and Forensic Capabilities



Source: Department of Defense Video and Imagery Distribution System. | [GAO-17-580](#)

The photographs above depict a warfighter obtaining a biometric iris image (left) and a forensic investigator collecting a latent fingerprint (right).

Abbreviations

ABIS	Automated Biometric Information System
CENTCOM	U.S. Central Command
DFBA	Defense Forensics and Biometrics Agency
DNA	Deoxyribonucleic Acid
DOD	Department of Defense
OCO	Overseas Contingency Operations
SOCOM	U.S. Special Operations Command
USD AT&L	Under Secretary of Defense for Acquisition, Technology, and Logistics

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



August 7, 2017

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

The Honorable Devin Nunes
Chairman
The Honorable Adam Schiff
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

During continued military operations in Iraq and Afghanistan, U.S. forces have faced an adversary that is often indistinguishable from innocent civilians in the general population. The Department of Defense (DOD) has relied on biometric and forensic capabilities to identify, target, and disrupt enemy combatants and terrorists in these countries and worldwide. Since 2008 DOD has used biometric and forensic capabilities to capture or kill 1,700 individuals, deny 92,000 individuals access to military bases, and identify and place 213,000 individuals on DOD's biometrically enabled watchlist.¹

Biometric capabilities are used to identify individuals based on measurable anatomical, physiological, and behavioral characteristics such as fingerprints, iris scans, and voice recognition. Forensic capabilities support the scientific analysis of evidence—such as deoxyribonucleic acid (DNA) and latent fingerprints—to link persons, places, things, and events, such as linking enemy combatants to explosives and firearms used to attack U.S. and coalition forces. DOD utilizes deployable biometric and forensic capabilities to support a range of military operations, such as targeting, force protection, and humanitarian assistance.

¹Hereinafter, annual dates are provided in calendar year unless otherwise specified.

DOD's deployable biometric and forensic capabilities were mainly developed through rapid acquisition processes and funded with Overseas Contingency Operations (OCO) funds—funds that were provided outside of DOD's base budget process. While DOD has previously taken steps to fund some of its deployable biometric and forensic capabilities in the base budget, these funding levels may not be adequate to ensure their continued availability. Moreover, through 2012, DOD had not developed comprehensive long-term requirements (hereinafter referred to as enduring requirements), such as policy, doctrine, and training, to ensure the long-term availability of deployable biometric and forensic capabilities.

We reported in 2011 that DOD could better conform to biometric collection standards and share biometric information with other federal agencies.² In 2012 we identified the need for additional biometric training for DOD leadership and more timely biometric transmission processes.³ Finally, in 2013 we found that additional planning and oversight were required for managing DOD's deployable forensic capabilities.⁴ Those three prior reports contained a total of 16 recommendations, and we discuss the implementation status of these recommendations later in this report.

House Report 114-537, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2017, and House Report 114-573, accompanying a bill for the Intelligence Authorization Act for Fiscal Year 2017, included provisions for us to review DOD's progress in establishing enduring deployable biometric and forensic capabilities.⁵ This report evaluates the extent to which DOD since 2011 has:

1. validated enduring requirements for deployable biometric and forensic capabilities;

²GAO, *Defense Biometrics: DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies*, [GAO-11-276](#) (Washington, D.C.: Mar. 31, 2011).

³GAO, *Defense Biometrics: Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics in Afghanistan*, [GAO-12-442](#) (Washington, D.C.: Apr. 23, 2012).

⁴GAO, *Defense Forensics: Additional Planning and Oversight Needed to Establish an Enduring Expeditionary Forensic Capability*, [GAO-13-447](#) (Washington, D.C.: June 27, 2013).

⁵H.R. Rep. 114-537, at 214-215 (2016); and H.R. Rep. 114-573, at 14-15 (2016).

-
2. taken actions to meet enduring requirements for deployable biometric and forensic capabilities and overcome any related challenges; and
 3. taken actions to address our prior recommendations regarding its biometric and forensic activities.

This report focuses on DOD's efforts to establish enduring biometric and forensic capabilities across DOD doctrine, organization, training, materiel, leadership and education, personnel, and facilities from 2011 to the present. We did not assess digital; multimedia; cyber; or chemical, biological, radiological, and nuclear forensic requirements and capabilities.⁶ For objective one, we identified and assessed relevant strategies, guidance, and plans, and we met with officials from across the department to determine DOD's validated enduring deployable biometric and forensic requirements. For objective two, we identified and evaluated relevant planning, acquisition, and sustainment documents, and we met with officials from across the department to discuss biometric and forensic capabilities and capability gaps. We also compared the content and process for developing DOD's biometric and forensic strategic plans against Standards for Internal Control in the Federal Government for control activities to determine their enterprise utility.⁷ In addition, we compared federal information systems guidance on contingency planning against acquisition planning and development documents for DOD's follow-on authoritative biometric database. For objective three, we evaluated actions taken by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and the military services to address our prior biometric and forensic recommendations, including issuance of new or updated guidance, policies, and plans. More detailed information on our scope and methodology can be found in appendix I of this report.

We conducted this performance audit from June 2016 to August 2017 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

⁶The Air Force and Defense Intelligence Agency have biometric and forensic responsibilities outside the scope of this review. Specifically, the Secretary of the Air Force is DOD's designated executive agent for digital and multimedia forensics, and the Director of the Defense Intelligence Agency is DOD's intelligence lead for biometric and forensic intelligence activities. We did not include intelligence agencies as part of this review.

⁷GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

DOD Biometric and Forensic Roles and Responsibilities

In April 2011 DOD issued a directive establishing a “defense forensic enterprise” that, among other things, provided policy and assigned responsibilities within the department to develop and maintain an enduring and holistic forensic capability to support the full range of military operations.⁸ In January 2016 DOD reissued a directive establishing a “defense biometrics enterprise” that, among other things, provided policies and assigned responsibilities within the department to provide a critical end-to-end biometric capability to support decision-making across the full range of military operations.⁹ These directives assigned USD(AT&L) responsibility for overseeing and coordinating the department’s biometric and forensic enterprise activities. USD(AT&L) utilizes the Defense Biometrics and Forensics Office to carry out its oversight and coordination responsibilities. The office coordinates and synchronizes biometric and forensic requirements, as well as facilitates the development and implementation of enterprise-wide policies.

In 2008 and 2011 the Secretary of Defense designated the Secretary of the Army as the executive agent for DOD’s biometric and forensic activities, respectively. In 2013 the Secretary of the Army designated the Defense Forensics and Biometrics Agency (DFBA) as the executive manager and tasked the agency with carrying out the Army’s biometric and forensic executive agent responsibilities, which include, among other things, leading enterprise coordination, acquiring common capabilities, ensuring that capabilities are planned and budgeted for, and overseeing and maintaining DOD’s authoritative biometric database through its Biometrics Operations Division. DFBA, in carrying out the Army’s forensics executive agent functions, also coordinates with the Army’s Criminal Investigations Command, which manages the Defense Forensic

⁸DOD Directive 5205.15E, *DOD Forensic Enterprise (DFE)* (Apr. 26, 2011).

⁹DOD Directive 8521.01E, *DOD Biometrics* (Jan. 13, 2016).

Science Center—the Army entity tasked with planning, programming, and providing joint or common forensic capabilities.

By directive, the Office of the Secretary of Defense, the Joint Staff, the military services, and the combatant commands are required to support various programs and policies within the biometric and forensic enterprises, such as coordinating and integrating requirements and capabilities to prevent unnecessary duplication. For example, the combatant commands are responsible for identifying, validating, and prioritizing theater-specific, joint biometric and forensic requirements while the military services and other DOD components plan, program, and field biometric and forensic capabilities to meet warfighter needs. The individual military services, the geographic combatant commands, and Special Operations Command (SOCOM) all have their own offices to oversee their biometric and forensic activities.

DOD's Requirements Validation and Rapid Acquisition Processes

DOD utilizes the Joint Capabilities Integration and Development System to identify, assess, prioritize, and validate joint military requirements, including deployable biometric and forensic requirements. The Joint Capabilities Integration and Development System process is overseen by the Joint Staff's Joint Requirements Oversight Council.¹⁰ Joint military requirement gaps are identified, typically by geographic combatant commands, and validated often by a military service or by the Joint Staff. DOD then studies potential non-materiel and materiel solutions to reduce or eliminate validated capability gaps. Non-materiel solutions include changes to doctrine, organization, training, or policy. Materiel solutions are items necessary to equip, operate, maintain, and support military activities, and they include biometric and forensic collection kits and communications equipment for transmitting biometric and forensic data to and from the warfighter. Potential materiel solutions are evaluated through an analysis-of-alternatives process whereby the performance,

¹⁰The Joint Requirements Oversight Council is chaired by the Vice Chairman of the Joint Chiefs of Staff and is comprised of senior representatives from each of the military services.

effectiveness, suitability, and estimated costs of potential materiel solutions are determined.¹¹

DOD has a rapid acquisition process to support urgent and emergent combatant commander needs during ongoing and anticipated contingency operations. Urgent and emergent operational needs are generated when other means—such as the department’s traditional requirements and acquisition processes—cannot be tailored to address operational requirements in a timely fashion.¹² A goal of the rapid acquisition process is to typically field a capability solution to an urgent or emergent operational need within 2 years. The rapid acquisition process is generally overseen by the Joint Staff and the Joint Rapid Acquisition Cell within the Office of the Secretary of Defense. Once a joint urgent or emergent operational need is validated by the Joint Staff, DOD may designate a sponsor—usually a military service—with responsibility for evaluating potential non-materiel and materiel solutions, and assigning a milestone decision authority to approve a solution and oversee its implementation.¹³

Deployable Biometric and Forensic Capabilities

Based on validated requirements to support a range of military operations, DOD has fielded a number of deployable capabilities to collect, analyze, match, transmit, store, and share biometric and forensic information.¹⁴

¹¹We have issued numerous reports discussing DOD’s joint requirements process. For example, see GAO, *Defense Acquisitions: DOD’s Requirements Determination Process Has Not Been Effective in Prioritizing Joint Capabilities*, [GAO-08-1060](#) (Washington, D.C.: Sept. 25, 2008); and GAO, *Defense Management: Guidance and Progress Measures Are Needed to Realize Benefits from Changes in DOD’s Joint Requirements Process*, [GAO-12-339](#) (Washington, D.C.: Feb. 24, 2012).

¹²A joint urgent operational need is driven by ongoing contingency operations, and a joint emergent operational need is driven by anticipated contingency operations. Joint Staff, *Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)* (Feb. 12, 2015).

¹³DOD Directive 5000.71, *Rapid Fulfillment of Combatant Commander Urgent Operational Needs* (Aug. 24, 2012); and, DOD Instruction 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015) (incorporating change 2, Feb. 2, 2017).

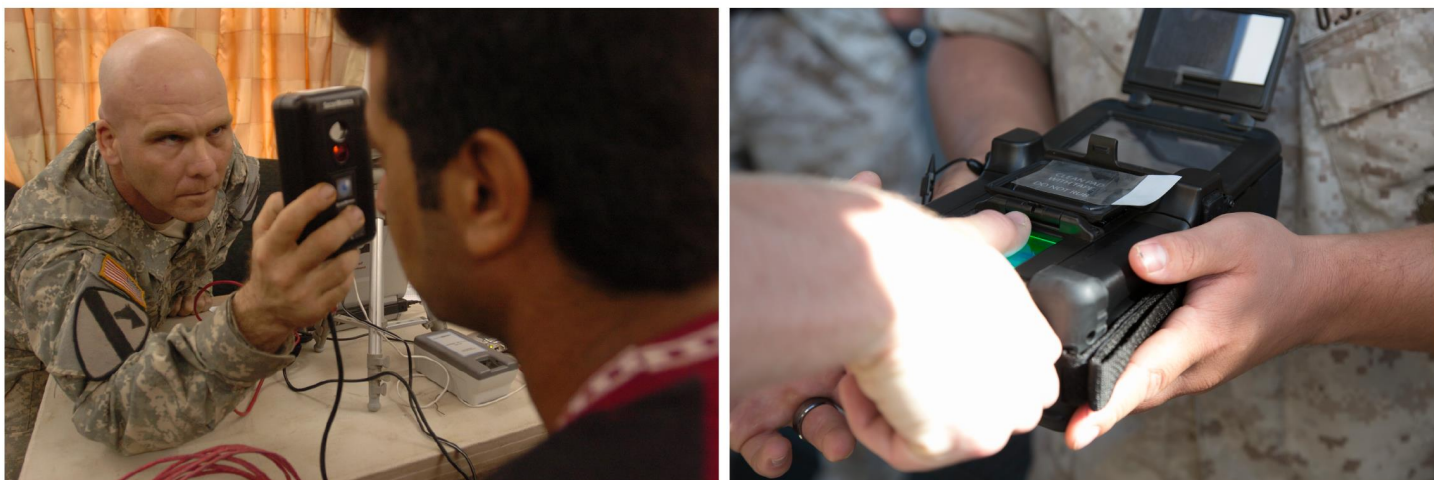
¹⁴DOD defines deployability as the ability to move forces and materiel anywhere in the world in support of a military operation. See DOD Instruction 4540.07, *Operation of the DOD Engineering for Transportability and Deployability Program* (Feb. 19, 2016).

Biometric collection capabilities include the following:

- **Secure Electronic Enrollment Kit:** Army, Navy, Marine Corps, and SOCOM hand-held device used to collect fingerprint, iris, facial images, and biographical information.
- **Biometrics Automated Toolset:** Army hand-held device and computer equipment used to collect (and transmit) fingerprint, iris, and facial images.
- **Identity Dominance System:** Navy and Marine Corps hand-held device and computer equipment used to collect (and transmit) fingerprint, iris, and facial images in both shore and maritime environments. The Navy and Marine Corps capabilities are separately managed, acquired, and funded through the individual services.
- **BioSled:** SOCOM hand-held device attached to a cellular phone used to collect fingerprint, iris, facial images, and biographical information.

For examples of biometric collection devices, see figure 1.

Figure 1: Biometric Automated Toolset and Secure Electronic Enrollment Kit Collection Devices in Use



Source: Department of Defense Video and Imagery Distribution System. | GAO-17-580

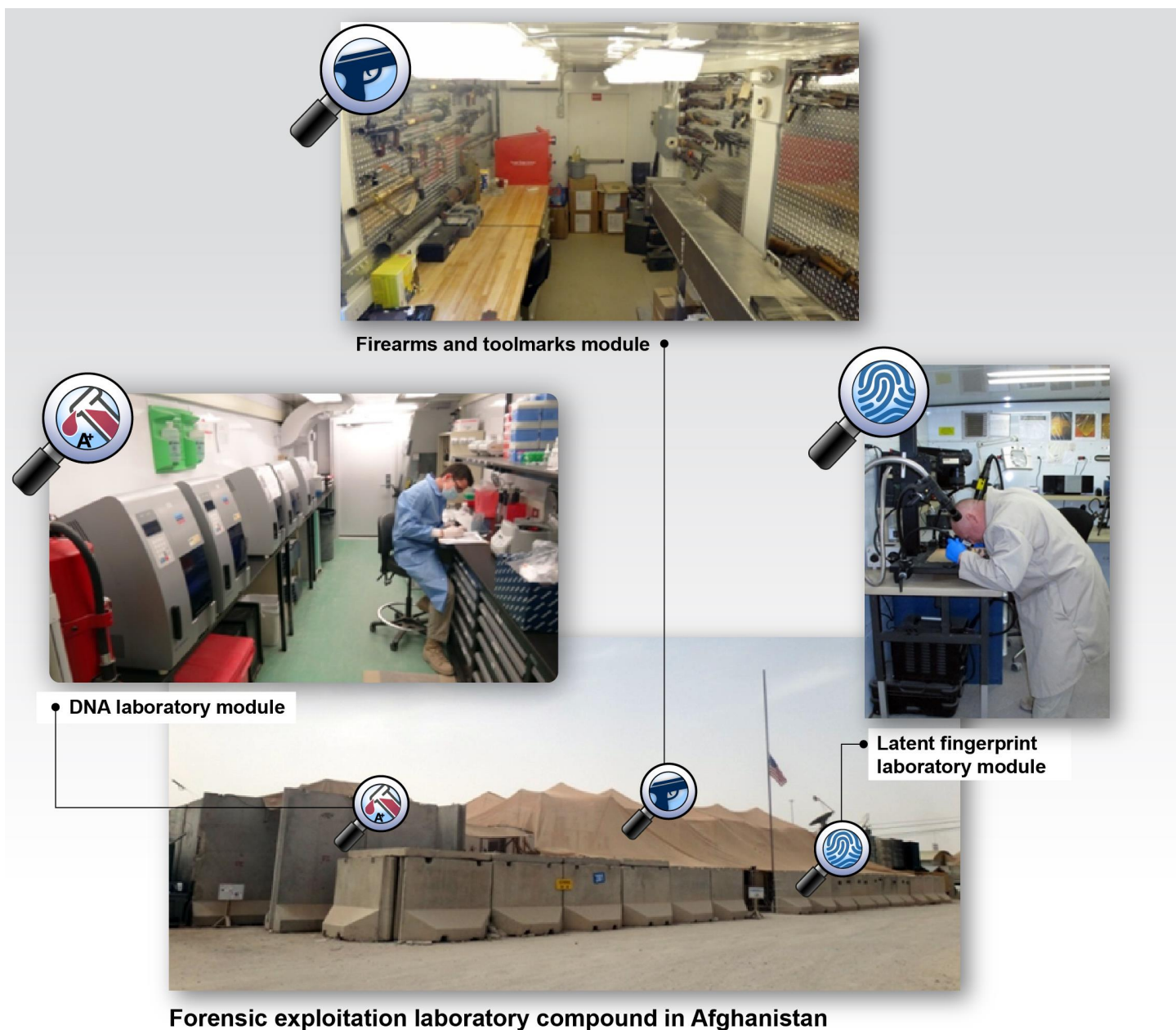
Forensic analysis capabilities include the following:

- **Exploitation Analysis Center:** SOCOM exploitation kit used to collect and process latent fingerprints and DNA samples, among other forensic material.

-
- **Expeditionary Forensic Exploitation Capability:** Marine Corps exploitation kit modeled after SOCOM's exploitation analysis center and used to collect and process latent fingerprints and DNA samples, among other forensic material.
 - **Forensic Exploitation Analysis Tool:** Managed by the Navy, this tool is a laboratory-information management and database sharing software system for documenting, tracking, reporting, and sharing forensic data.¹⁵
 - **Forensic Exploitation Laboratories:** Owned and operated by the Army's Defense Forensics Science Center, these laboratories provide a modularized, scalable capability to forensically analyze latent fingerprints, DNA, explosives, drugs, and firearm and tool marks. The Army has also established a "reachback" operations center at the Gillem Enclave, Georgia, to oversee the deployment and management of the forensic exploitation laboratories, and to provide expertise and analytical capabilities to process forensic material (see figure 2).

¹⁵The Forensic Exploitation Analysis Tool was formerly known as the Weapons Technical Intelligence Exploitation Analysis Tool.

Figure 2: Examples of Forensic Exploitation Laboratory Modules




Source: Defense Forensics Science Center. | GAO-17-580

Biometric and forensic transmission, storage, and sharing capabilities include the following:

-
- **DOD Automated Biometric Information System (DOD ABIS):** DOD ABIS is the department's authoritative biometric repository for non-U.S. persons. It supports the storing, matching, and sharing of biometric data collected as part of military operations, including fingerprint, iris, palm, facial images, and biographical information, as well as forensically collected latent fingerprint information. Biometric submissions and match requests are prioritized for processing based on agreements between DFBA and the submitting organization.¹⁶ Figure 3 shows a person of interest whom DOD identified through biometric data that were collected, analyzed, and stored in DOD ABIS.


¹⁶There are five levels of prioritization for processing DOD ABIS submission and match requests that in fiscal year 2016 ranged from a 5-minute to a 4-hour response time, as reported by Army officials.

Figure 3: Example of Biometrics Used to Identify a Person of Interest




UNCLASSIFIED

HIT OF THE WEEK 14 Apr 17




BAT Enrollment: Jun 7, 2006

Name: [REDACTED]
 TOT: DPRS
 POB: IQ
 DOB: [REDACTED]
 HGT: 000
 WGT: 000
 RFP: ID Badge
 Personnel Type: Other




BAT Enrollment: Jul 8, 2006

Name: [REDACTED]
 TOT: CAR
 POB: IQ
 DOB: [REDACTED]
 HGT: 5' 05"
 WGT: 135
 ASL: Terrorism ACF/AIF
 Personnel Type: Enemy Combatant



SOCOM Enrollment: Mar 30, 2017

Name: [REDACTED]
 TOT: CPDR
 POB: XX
 DOB: Not in File
 HGT: 000
 WGT: 000
 ASL: Suspected of Terrorist Activities
 Personnel Type: Not in File



ALERT CATEGORIES: [REDACTED]

BLUF: *An individual on the U.S. DoD BEWL was encountered by Coalition Forces during a military operation.*

- On Jun 7, 2006, the subject was enrolled for an ID Badge request in Fallujah, Iraq. The biometric file, containing the subject's fingerprints, was submitted to the DoD Authoritative Biometric Repository where it did not match any previous enrollments and was retained for future searches.
- On Jul 8 2006, the subject was detained by Coalition Forces (CF) near Baghdad, Iraq, for acts of terrorism and attacks against CF. His biometric file, including face, iris, and fingerprint images, were submitted to the DoD Authoritative Biometric Repository where it matched his previous enrollment. The subject was subsequently nominated and approved to the U.S. DoD Biometrically Enabled Watchlist (BEWL) based on the nature of his enrollment.
- On Mar 30 2017, the subject was encountered during a military operation in Iraq by CF and detained for suspicion of terrorist activities. His biometrics were collected and the file, containing face and fingerprint images, were uploaded to the SOFEX portal, submitted to the DoD Authoritative Biometric Repository, where it matched his previous enrollments and to the DoD BEWL.

This match highlights the important role the DoD Biometrics Enterprise plays in identifying an individual against multiple encounters of different nature. This match also demonstrates the importance of continued biometric collections and the DoD Biometrics Enterprise's ability to identify threats and protect U.S. interests.

Alert Detail: [REDACTED]

Source: Defense Forensics and Biometrics Agency. | GAO-17-580

- **Special Operations Forces Exploitation:** SOCOM communications architecture utilizing global satellite networks to transmit biometric and forensic information through an online portal to and from DOD ABIS with match/no-match responses.
- **Department of the Navy Identification and Screening Information System:** Navy and Marine Corps communications architecture to transmit biometric information through an online portal to and from DOD ABIS with match/no-match responses. The system is modeled after SOCOM's Special Operations Forces Exploitation capability.

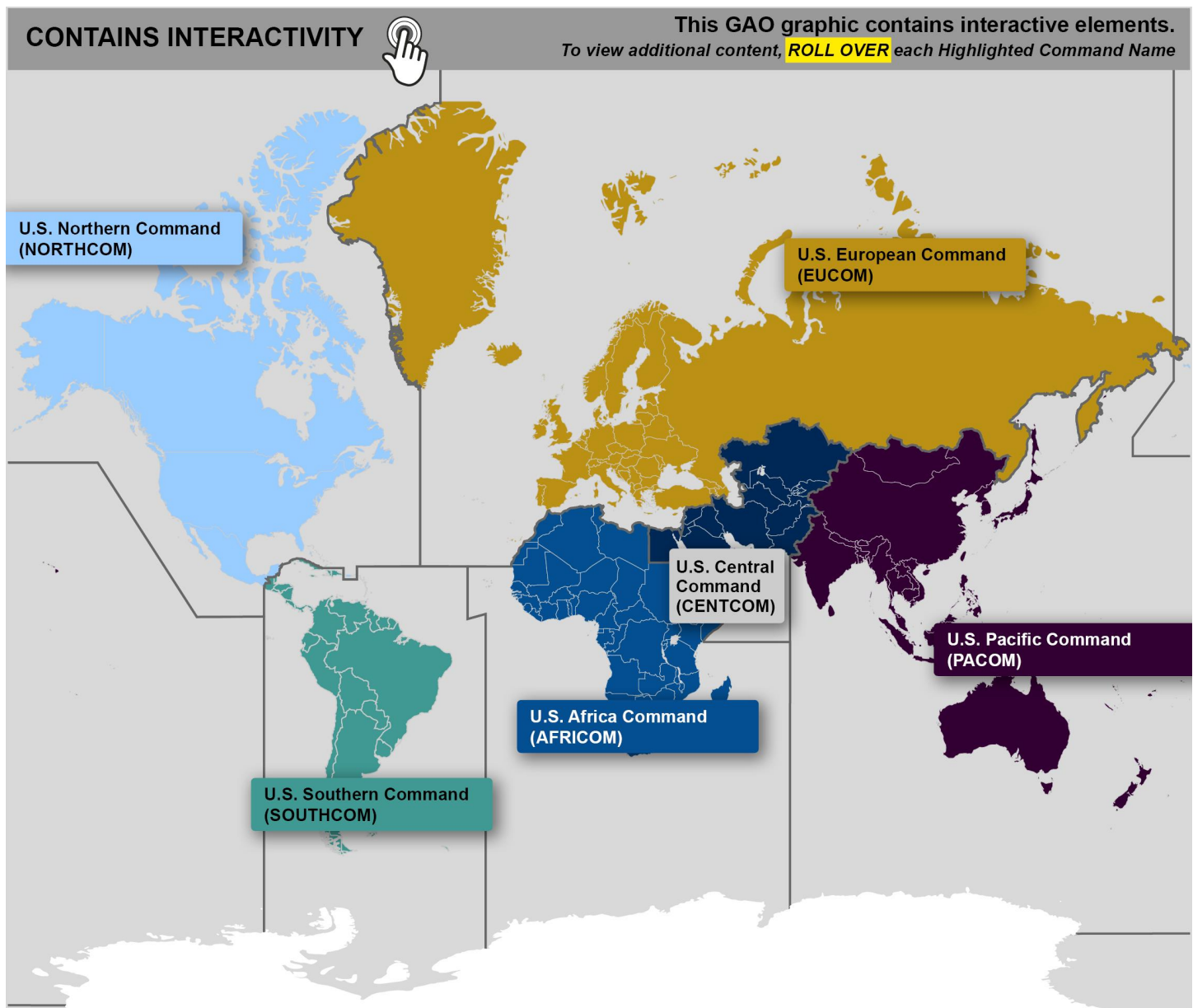
-
- **Near Real Time Identity Operations:** Army-provided regional forward server, communications platform, and collection devices that are fielded in U.S. Central Command's (CENTCOM) area of responsibility in response to a 2014 CENTCOM joint emergent operational need. In September 2014 CENTCOM submitted a joint emergent operational need to meet 21 command-specific requirements.¹⁷ In November 2014 the Joint Requirements Oversight Council validated CENTCOM's operational need and directed the executive agent to establish it as an enduring capability. In January 2015 the Joint Rapid Acquisition Cell assigned the Army as the office of primary responsibility for fulfilling the need.

DOD Has Validated Enduring Requirements for Deployable Biometric and Forensic Capabilities

DOD has validated enduring non-materiel and materiel requirements for deployable biometric and forensic capabilities. DOD officials emphasized the importance of this step, given DOD's increasing operational demand for biometric and forensic capabilities, as shown in figure 4—an interactive graphic—and in appendix II.

¹⁷CENTCOM Joint Emergent Operational Need, *USCENTCOM Near Real Time Identity Operations Support to Joint Operations* (Sept. 8, 2014) (FOUO).

Figure 4: Geographic Combatant Commands' Demand for Biometric and Forensic Capabilities



Source: GAO analysis of Department of Defense information. | GAO-17-580

DOD Has Validated Non-materiel Enduring Requirements for Deployable Biometric and Forensic Capabilities

To better support current and anticipated warfighter demand, DOD validated 30 non-materiel enduring requirements for deployable biometric and forensic capabilities, as shown in table 1.

Table 1: Department of Defense (DOD)-Validated, Non-materiel Enduring Requirements for Deployable Biometric and Forensic Capabilities, by Area

Area	Number of Validated Requirements	Example
Doctrine	9	Develop and update joint doctrine
Organization	3	Establish working groups
Training	6	Integrate biometrics and forensics into joint training
Leadership & Education	2	Integrate biometrics and forensics into leader training
Personnel	1	Develop training requirements
Policy	9	Develop DOD biometric and forensic guidance

Source: GAO analysis of Defense Forensics and Biometrics Agency documentation. | GAO-17-580.

These requirements are designed to transition DOD's biometric and forensic capabilities, over a multi-year period, from rapidly acquired and OCO-funded capabilities to enduring capabilities that are resourced through base funding. According to DOD officials, the 30 non-materiel requirements remain current and comprehensive, as of May 2017. We found that each biometric and forensic non-materiel requirement was submitted by the Army, as DOD's executive agent for biometrics and forensics; coordinated across the department; and approved and documented by the Joint Requirements Oversight Council in August 2013 and November 2014, respectively.

DOD Has Validated Materiel Enduring Requirements for Deployable Biometric and Forensic Capabilities

DOD has validated several materiel enduring requirements for deployable biometric and forensic capabilities that facilitate the recognition, collection, preservation, analysis, transmission, matching, storage, and sharing of biometric and forensic data. While DOD does not have a consolidated list of its validated biometric and forensic materiel requirements at this time, it is in the process of developing such a list.

DOD's materiel requirements are currently described in department, military service, and SOCOM strategies and acquisition documents, and in geographic combatant command operational plans. For example, the 2012 Marine Corps Identity Strategy identified a requirement for biometric and forensic collection, transmission, and storage capabilities to support operations globally.¹⁸ Additionally, the Army identified enduring requirements for DOD's authoritative biometric database in documents such as its draft 2016 capability production document and its 2015 analysis of alternatives.¹⁹

DOD Has Taken Actions to Meet Enduring Biometric and Forensic Requirements but Faces Challenges in Sustaining Progress

DOD has made significant progress in addressing 7 of the 30 validated non-materiel enduring requirements for deployable biometric and forensic capabilities. The military services and SOCOM have also taken actions to ensure the continued availability of several deployable materiel biometric and forensic capabilities to meet enduring requirements. However, DOD's efforts to institutionalize deployable biometric and forensic capabilities are limited by strategic planning gaps and acquisition management challenges.

DOD Is Addressing Non-materiel Enduring Requirements for Deployable Biometric and Forensic Capabilities

DOD has made significant progress in addressing 7 of the 30 validated non-materiel requirements for biometric and forensic capabilities that were identified in 2013 and 2014, as shown in table 2.

¹⁸U.S. Marine Corps, *USMC Identity Operations Strategy 2020* (Aug. 14, 2012).

¹⁹U.S. Army, *Biometric Enabling Capability Analysis of Alternatives* (2015); and U.S. Army, *Draft Capability Production Document for Next Generation Automated Biometric Identification System* (Feb. 8, 2016).

Table 2: Non-materiel Biometric and Forensic Requirements Reflecting Significant Progress as Assessed by the Defense Forensics and Biometrics Agency, by Area^a

	Area	Requirement	Department of Defense (DOD)-reported Completion Status
Doctrine	Biometrics	Develop a multi-service tactics, techniques, and procedures manual	100 percent
	Biometrics	Develop a stand-alone joint publication to support military operations	100 percent
Training	Biometrics	Integrate biometrics into DOD's joint training tasks	75 percent
Leadership and Education	Biometrics	Integrate tenets of biometrics into professional military education	75 percent
Policy	Biometrics	Publish a revised version of DOD Directive 8521.01E, <i>Department of Defense Biometrics</i>	100 percent
	Biometrics	Develop and publish a security classification guide	100 percent
	Forensics	Develop and publish a security classification guide	90 percent

Source: GAO analysis of Defense Forensics and Biometrics Agency documentation. | GAO-17-580

^aStatus information was provided by the Defense Forensics and Biometrics Agency. GAO discussed and confirmed the accuracy of this information with Joint Staff, Army Training and Doctrine Command, and Defense Forensics and Biometrics Agency officials.

According to DFBA documentation, DOD is in the process of addressing the remaining 23 non-materiel requirements, but as of May 2017 their status was below 75 percent complete. DFBA is leading DOD's effort to address all 30 validated non-materiel requirements, and it has prioritized and established timeframes for their completion by 2020, as directed by the Joint Requirements Oversight Council. DFBA officials told us that they initially focused on doctrine requirements, such as issuing Joint Doctrine Note 2-16, Identity Activities, and integrating biometric and forensic activities into existing joint publications, to better address training and policy requirements.²⁰ Appendix III includes a description of all 30 validated non-materiel enduring requirements by area, status, and anticipated completion, as of May 2017.

²⁰Joint Doctrine Note 2-16, *Identity Activities* (Aug. 3, 2016).

DOD Has Developed Materiel Biometric and Forensic Capabilities to Meet Several Enduring Requirements and Has Made Progress in Transitioning These Capabilities to Base Funding

DOD has developed biometric and forensic capabilities to meet several validated enduring materiel requirements, and it has made progress in transitioning these capabilities from OCO to base funding. The military services and SOCOM have initiated acquisition and sustainment programs, based on validated requirements, to ensure the continued availability of several materiel biometric and forensic capabilities, including the following:

- **Army Next Generation Biometric Collection Device.** The Army has initiated an acquisition program to identify a follow-on capability for its existing biometric collection device, the Biometrics Automated Toolset, which is scheduled to reach end-of-life in 2022, according to Army officials.²¹ The Army is conducting an analysis of alternatives to be completed at the end of fiscal year 2017 to inform its decision, according to the same officials.
- **Biometric Enabling Capability** (*hereinafter referred to as the DOD ABIS follow-on system*). In 2015 the Army completed an analysis of more than 10 alternatives to inform DOD's decision regarding a DOD ABIS replacement. DOD ABIS is scheduled to be replaced in fiscal year 2022.
- **Forensic Exploitation Laboratories.** Army officials expect to transition these laboratories to an enduring, base-funded capability in 2019. Officials from the Defense Forensics Science Center noted that the Army's draft expeditionary forensic strategy calls for an expeditionary lab to be aligned with each of the six geographic combatant commands.
- **Identity Dominance System.** The Navy and Marine Corps are jointly pursuing a replacement for their existing biometric collection device, the Secure Electronic Enrollment Kit, which, according to Navy and Marine Corps officials, is scheduled to reach end-of-life in 2019.

²¹"End-of-life" is a term DOD uses to indicate that support for a capability will no longer be available from any source.

-
- **SOCOM Biometric Collection Device.** SOCOM has initiated an acquisition program to replace its existing Secure Electronic Enrollment Kit and BioSled collection devices, which currently fulfill validated requirements. SOCOM officials anticipate that the replacement capability will be available in 2019.

DOD officials stated that the department has made progress in transitioning enduring biometric and forensic materiel capabilities from OCO to base budget funding. For example, Army officials stated that DOD ABIS has transitioned from a combination of OCO and base budget funding to an enduring capability funded through DOD's base budget. The Navy, Marine Corps, and SOCOM have also developed comprehensive programs of record for their biometric and forensic materiel capabilities that are expected to be funded through their respective base budgets. In addition, the Army anticipates transitioning its forensic exploitation laboratories from OCO to base funding by 2019. Officials from across DOD noted the importance of continuing to transition biometric and forensic materiel capabilities from OCO to base funding, to better ensure their continued availability.

DOD's Efforts to Institutionalize Deployable Biometric and Forensic Capabilities Are Limited by Strategic Planning Gaps and Acquisition Management Challenges

DOD's efforts to institutionalize its enduring deployable biometric and forensic capabilities are limited by strategic planning gaps and acquisition management challenges. These limitations include the absence of a current biometric strategic plan and supporting implementation plan, the absence of acquisition professionals to oversee CENTCOM's Near Real Time Identity Operations solution, the absence of a geographically dispersed DOD ABIS back-up capability, and difficulties in hiring and retaining qualified personnel to operate and maintain DOD ABIS.

DOD Lacks Current Biometric Strategic Planning Documents

While DOD has a current and approved forensic strategic plan, it does not have a current and approved biometric strategic plan. According to Standards for Internal Control in the Federal Government, strategic plans set the goals and objectives for an entity to achieve more effective and efficient operations and to minimize waste.²² Furthermore, the standards

²²[GAO-14-704G](#).

call for set goals and objectives to be reviewed periodically and updated as necessary.

In 2015 DOD issued a forensic strategic plan to guide its forensic enterprise through fiscal year 2020. The plan identifies several goals and objectives, such as enhancing enterprise effectiveness and information-sharing. DOD also issued a supporting forensic implementation plan in 2015 that includes strategic planning elements for each of the objectives, such as intended outcomes, measures of effectiveness, and assigning offices of primary responsibility. According to USD(AT&L) officials, the forensic strategic plan plays a critical role in focusing and prioritizing DOD's forensic enterprise activities.

In contrast, DOD's biometric strategic plan is out of date, and the department has not developed a supporting implementation plan. Specifically, DOD issued a biometric strategic plan in 2008, covering the 2008 – 2015 timeframe. The plan identifies several goals and objectives, such as institutionalizing biometric capabilities and coordinating biometric efforts across the department more effectively. The plan includes a requirement to be reviewed annually and updated as necessary. The plan also directs that a supporting implementation plan be developed. However, according to DOD officials, the biometric strategic plan has not been reviewed or updated since 2008, and a supporting implementation plan has not been issued. USD(AT&L), Army, Navy, Marine Corps, and DFBA officials agreed that the biometric strategic plan should be updated and a supporting implementation plan issued to better focus and prioritize enterprise goals and objectives for matters such as doctrine and policy, coordination, and acquisition and sustainment efforts. For example, DOD officials noted that the military services and SOCOM have a number of ongoing biometric acquisition and sustainment initiatives that are not articulated and synchronized in a single document, and that including information about these initiatives in an updated biometric strategic plan would enhance long-range enterprise planning.

According to DOD officials, the 2008 biometric strategic plan has not been reviewed and updated, and a supporting implementation plan has not been issued, because no organization has been assigned responsibility for completing these tasks. Further, these officials stated that if an entity were to independently undertake these tasks without being assigned to do so, there likely would be mixed acceptance across the enterprise. Without a strategic plan that identifies goals and objectives and a supporting implementation plan that identifies outcomes, measures of effectiveness, and responsibilities, among other things, DOD may be

missing an opportunity to reprioritize and better align enterprise efforts in important areas such as acquisition and sustainment.

DOD Faces Biometric and Forensic Acquisition Management Challenges

DOD's acquisition management challenges that are specific to its biometric and forensic enterprises include the absence of a milestone decision authority to oversee CENTCOM's Near Real Time Identity Operations solution, the absence of a geographically dispersed DOD ABIS back-up capability, and difficulties in hiring and retaining qualified personnel to operate and maintain DOD ABIS.

- **CENTCOM's Near Real Time Identity Operations solution lacks a milestone decision authority supported by acquisition professionals.** According to DOD officials, the Army could have more thoroughly considered existing, viable, and potentially less costly alternatives to address CENTCOM's 2014 operational need for a Near Real Time Identity Operations capability. In 2015 SOCOM offered the Army its Special Operations Forces Exploitation capability as a potential solution. According to military service, SOCOM, and DFBA documentation and officials, SOCOM's capability was a proven, highly effective, and cost-efficient communications architecture that met many of CENTCOM's 21 operational need requirements, including the ability to transmit and receive a match/no-match response from DOD ABIS within 3 minutes. Navy and Marine Corps officials stated that they modeled their communication architecture (i.e., the Department of the Navy Identification and Screening Information System) on the Special Operations Forces Exploitation capability, based on its demonstrated high performance and reliability. Other Army officials noted that the Army's fielded Biometrics Automated Toolset capability could potentially have been leveraged to satisfy some of CENTCOM's operational need requirements.

When CENTCOM's joint emergent operational need was validated by the Joint Staff and assigned by the Joint Rapid Acquisition Cell, the Army office responsible for overseeing the Near Real Time Identity Operations solution was given 90 days to identify and field a potential solution; thus, according to DOD officials, they had limited time to thoroughly assess alternative options. Army officials observed that while they discussed the feasibility of the Special Operations Forces Exploitation capability and other potential solutions with DOD, military service, and SOCOM officials in 2015, they rejected these alternatives because they did not meet all of CENTCOM's requirements, including

the ability to share unclassified information with allied partners and the ability to transmit and receive all match/no-match responses within 3 minutes.

While we did not, in the following assessments, validate the findings or the Army's efforts to address the corresponding deficiencies identified in them, the assessments highlight concerns within DOD regarding the performance of the Near Real Time Identity Operations solution. In June 2016 the Center for Naval Analyses issued an analysis of biometric and forensic data collected through November 2015 which examined several DOD information systems and found that the Near Real Time Identity Operations solution produced inconsistent match/no-match responses due to data synchronization challenges that could increase risk for existing and future missions conducted in the CENTCOM area of responsibility. In September 2016 the Army completed its operational assessment of the Near Real Time Identity Operations solution and found that it provided inconsistent match/no-match responses that "reduced warfighter confidence in the system." Based on their lack of confidence in the system, SOCOM and the Marine Corps sought and received approval for their forces in the CENTCOM area of responsibility to use their existing capabilities instead of the Near Real Time Identity Operations solution. Marine Corps officials asserted that the Near Real Time Identity Operations solution continued to provide incomplete match/no-match data as of May 2017. Army officials acknowledged that the Near Real Time Identity Operations solution operational assessment identified major deficiencies; however, they stated that the Army had addressed the major deficiencies as of May 2017. In addition, CENTCOM determined that the solution has military utility, and CENTCOM is interested in pursuing further enhancements to meet all of its 21 operational need requirements.

According to DOD Instruction 5000.02, a milestone decision authority, supported by acquisition professionals, will be assigned to oversee a rapid acquisition program such as the Near Real Time Identity Operations solution. The milestone decision authority is responsible for, among other things, overseeing the evaluation of alternative existing technologies to consider cost, schedule, performance, and operational risk before selecting a solution.²³ However, according to DOD officials, the Army did not assign a milestone decision authority and also did not assign an office with experienced acquisition

²³DOD Instruction 5000.02.

professionals to oversee the Near Real Time Identity Operations solution. DOD acquisition officials noted that if acquisition professionals had overseen the solution, they might have considered different performance, cost, or schedule trade-offs, which may have resulted in a different outcome. In 2015 DOD officials informed the Army of the need to assign a milestone decision authority, but as of May 2017 the Army had not assigned such an authority. Some Army officials told us that the office currently responsible for overseeing the Near Real Time Identity Operations solution has provided sufficient oversight.

According to DOD guidance, no later than 1 year after a system enters operation and sustainment, DOD should complete a disposition analysis that recommends a course of action, including whether to retain the system.²⁴ Given the absence of a milestone decision authority and the acquisition and performance challenges incurred with the Near Real Time Identity Operations solution, we believe that the department could benefit from a disposition analysis that is completed before the solution reaches operation and sustainment. A disposition analysis not only would inform DOD's management of the Near Real Time Identity Operations solution, but also would inform the department's other biometric and forensic acquisition programs, such as the DOD ABIS follow-on system.

- **DOD ABIS lacks a geographically dispersed back-up capability.** DOD's mission-critical authoritative biometrics database (i.e., DOD ABIS) faces heightened operational risk because it does not have a geographically dispersed back-up capability. According to officials from across the biometric enterprise, U.S. forces rely on DOD ABIS to store and match biometric and latent fingerprint information. Without a geographically dispersed back-up, there is increased risk that if DOD ABIS were unavailable for unexpected and extended periods, U.S. forces would be unable to receive timely match/no-match information to identify enemy combatants and terrorists.

DOD ABIS has a partial back-up system that is located less than 20 miles away from its primary site in West Virginia, thereby making it vulnerable to many of the same natural and man-made disasters to which the primary site is vulnerable. According to the National Institute of Standards and Technology, mission-critical information systems, such as DOD ABIS, should have a back-up capability located in a geographic area that is unlikely to be affected by the same hazards as

²⁴DOD Instruction 5000.02.

the primary site.²⁵ The Army, which has responsibility for operating and maintaining DOD ABIS, considered geographic dispersal as part of the 2015 DOD ABIS follow-on system analysis of alternatives. However, according to DOD officials, the Army has not included geographic dispersal as part of the selection criteria for the DOD ABIS follow-on system.

When the Army fielded DOD ABIS in 2004 it was responding to a CENTCOM urgent need to support military operations, and therefore it focused on rapidly fielding an initial capability, according to DOD officials. At that time the Army did not develop a geographically dispersed DOD ABIS back-up capability, and it has not subsequently developed such a capability because of anticipated costs and the assumption that the existing back-up system suffices, according to DOD officials. However, DOD officials stated that the Army has an opportunity to consider the pros and cons of developing a geographically dispersed capability as part of the DOD ABIS follow-on system acquisition program. For example, one of the options under consideration entails transitioning DOD ABIS's data to a virtual cloud format. According to DOD officials, doing so could reduce the operational risk associated with having limited geographic dispersal.

- **DOD's contractors face challenges in hiring and retaining qualified personnel to operate and maintain DOD ABIS.** DOD ABIS's operational risk is exacerbated by DFBA's challenges in hiring and retaining qualified personnel to operate and maintain the system. DFBA's Biometrics Operations Division is responsible for managing DOD ABIS's day-to-day operations and uses contractors to support several services, including information technology security, staffing an around-the-clock watch desk to support warfighter requirements, and providing latent fingerprint examiners to adjudicate potential fingerprint matches when automated determinations are not definitive, according to officials. However, DFBA officials stated that its contractors have experienced difficulty in hiring and retaining staff for these functions because the current support contracts were issued using a lowest-price technically acceptable source selection process—that is, awarding contracts to the lowest bidder deemed technically qualified. This contracting approach limits DOD's ability to attract bids from companies with less restrictive compensation, according to DOD officials. In contrast, a tradeoff contracting approach permits tradeoffs among cost and non-cost factors and

²⁵National Institute for Standards and Technology, *NIST Special Publication 800-34 Rev 1: Contingency Planning Guide for Federal Information System* (May 2010).

allows a contract to be awarded to a contractor that is not the lowest bidder. According to DOD officials, a tradeoff approach could enhance the quality of contract offers and improve contractor hiring and retention through better compensation. According to DOD acquisition officials, a lowest-price technically acceptable approach should be used for basic services, such as sanitation and landscaping, and not for technical, highly-skilled services, such as information technology security and latent fingerprint examination.

DFBA pursued a tradeoff approach for its DOD ABIS mission-critical functions, but a lowest-price technically acceptable approach was settled upon by Army Contracting Command, according to DFBA and Army Contracting Command officials. Specifically, DFBA's inability to attain a tradeoff approach was caused by difficulty in completing required documentation, such as detailed job position descriptions, in a timely manner, despite DFBA's and Army Contracting Command's combined efforts.

The National Defense Authorization Act for 2017 directs DOD to avoid the use of lowest-price technically acceptable selection criteria to acquire knowledge-based professional services such as information technology, cybersecurity, systems engineering, and technical assistance to the maximum extent practicable.²⁶ Although the current DOD ABIS support contracts pre-date the passage of the Act, USD(AT&L) and DFBA officials stated that daily operation and maintenance of DOD ABIS are considered knowledge-based professional services that require highly skilled personnel to perform and therefore, consistent with the Act, the department should consider pursuing a tradeoff contracting approach when it is practicable to do so, such as during future contract solicitations. Standards for Internal Control in the Federal Government emphasizes the importance of recruiting, developing, and retaining competent personnel. DFBA's ability to provide timely and authoritative match/no-match responses to U.S. forces engaged in ongoing operations might be negatively affected if its contractors cannot hire and retain sufficient numbers of highly skilled personnel to operate and maintain DOD ABIS's mission-critical functions.

²⁶Pub. L. No. 114-328, div. A, title VIII, subtitle C, § 813(c) (Dec. 23, 2016).

DOD Has Implemented Almost All of Our Prior Biometric- and Forensic-related Recommendations

In our prior reports on DOD's biometric and forensic activities issued since 2011, we made 16 recommendations to enhance the biometric and forensic enterprises. As of May 2017, DOD had implemented 15 of the 16 recommendations and was making progress toward implementing the remaining recommendation, as shown in table 3.²⁷ The 15 closed recommendations and additional steps DOD has taken since they were closed are summarized in appendix IV.

Table 3: Status of the Department of Defense's (DOD) Implementation of Our Biometric and Forensic Recommendations since 2011, as of May 2017

GAO Report Number	Report Title	Recommendations		
		Total	Implemented	Not implemented
GAO-11-276	Defense Biometrics: DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies	5	5	0
GAO-12-442	Defense Biometrics: Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics in Afghanistan	7	6	1
GAO-13-447	Defense Forensics: Additional Planning and Oversight Needed to Establish an Enduring Expeditionary Forensic Capability	4	4	0
Report totals		16	15	1

Source: GAO analysis of DOD information. | GAO-17-580

In March 2011 we found that a biometric collection device used primarily by the Army did not meet DOD-adopted standards; and that DOD did not have a finalized biometric information-sharing agreement with the Department of Homeland Security; and we identified concerns that DOD ABIS might be unable to meet the search demands of non-DOD biometric systems.²⁸ We made five recommendations addressing DOD's process and policies for updating and testing collection devices and improving information-sharing across federal agencies. DOD has implemented each of these recommendations. For example, in January 2016 DOD updated

²⁷ [GAO-11-276](#), [GAO-12-442](#), and [GAO-13-447](#).

²⁸ [GAO-11-276](#).

its biometric directive that, among other things, now assigns responsibility for ensuring that its biometric-related systems conform to federal standards. In addition, in January 2016 the Assistant Secretary of Defense for Homeland Defense and Global Security, in coordination with the Department of Homeland Security, updated guidance to further improve the sharing of biometric, biographical, and identity-management data between the two departments for screening and identity-verification purposes.

In April 2012 we found that biometric training for leaders did not provide instruction on the effective use of biometrics; several factors during the data transmission process limited the use of biometrics in Afghanistan; and requirements did not exist for DOD to disseminate biometric lessons learned across the department.²⁹ We made seven recommendations to address these findings, six of which the department has implemented. For example, between February 2015 and January 2017 DOD approved 25 new universal joint tasks that relate to biometric and forensic training.³⁰ This action is one of the first steps DOD must take in order to institutionalize biometric-related training and education to support its operational requirements. With respect to the recommendation that is not implemented, DOD officials told us that the department is taking actions to address several data transmission factors that hindered the Army's and Marine Corps' ability to identify (and capture) enemy combatants in Afghanistan in a timely manner. These factors include mountainous terrain, competing demands for communications infrastructure, and delays in updating hand-held biometric collection devices with the most current biometrically enabled watchlist. During this review, USD(AT&L) and military service officials told us that these data transmission factors will be analyzed and potentially addressed through the DOD ABIS follow-on system acquisition program and the CENTCOM Near Real Time Identity Operations solution.³¹ We believe that these actions will address

²⁹[GAO-12-442](#).

³⁰The universal joint task list is a menu of foundational tasks for joint operations planning across the range of military operations. These approved tasks contain the basic language for identifying and developing agency and joint mission-essential tasks that are based on supported command mission capability requirements and inform the development of joint training programs and training objectives, among other things. See Chairman of the Joint Chiefs of Staff Instruction 3500.02B, *Universal Joint Task List Program* (Jan. 15, 2014).

³¹Army Program Executive Officer Enterprise Information Systems Memorandum, *Biometrics Enabling Capability (BEC) Increment (Inc) 0 Acquisition Decision Memorandum (ADM)* (Feb. 17, 2016).

the intent of our 2012 recommendation. DOD officials also stated that they have improved the reliability and responsiveness of DOD ABIS. From fiscal years 2014 through 2016, DOD ABIS was available more than 98 percent of the time, excluding brief scheduled periods of unavailability for system updates and planned maintenance actions. Additionally, in fiscal year 2016 DOD ABIS's average match/no-match response time was generally between 1 and 11 minutes, depending on the prioritization level assigned to the biometric submission.

In June 2013 we found that DOD's draft forensic strategic plan was missing important elements such as milestones and metrics to gauge progress; that USD(AT&L) had not reviewed and evaluated military service and SOCOM budget estimates, as required by DOD's forensic directive; and that DOD had not provided guidance to the military services on how they were to collect and report forensic budget data to USD(AT&L).³² We made four recommendations addressing DOD's forensic strategic plan and the review and evaluation of forensic budget estimates. DOD has implemented each of these recommendations. For example, DOD issued a forensic enterprise strategy in March 2015 and a supporting implementation plan in September 2015. The strategic plan and implementation plan, when viewed together, contain several important elements for effective strategic planning, including goals, milestones, and metrics.

Conclusions

DOD relies on its deployable biometric and forensic capabilities to support a range of military operations, including the identification and targeting of enemy combatants and terrorists. Since 2011 DOD has made considerable progress in institutionalizing these capabilities, the majority of which were developed through rapid acquisition processes and funded with OCO funds to meet urgent and emergent warfighter needs in Iraq and Afghanistan. For example, DOD has validated a number of non-materiel and materiel enduring requirements, and several of the resulting capabilities have transitioned, or are in the process of transitioning, from OCO to base funding. Furthermore, DOD has implemented almost all of our prior biometric- and forensic-related recommendations that we believe are consistent with the department's efforts to institutionalize its

³²[GAO-13-447](#).

deployable biometric and forensic capabilities. However, DOD's continued success could be diminished by gaps in strategic planning documents and acquisition management challenges. Specifically, without a current biometric strategic plan and supporting implementation plan, DOD is not well positioned to prioritize and focus enterprise-wide activities. Furthermore, without a milestone decision authority to oversee DOD's development of a Near Real Time Identity Operations solution, and a disposition analysis to recommend a path forward, DOD risks facing continued cost, schedule, and performance issues. Lastly, the ability of DOD ABIS to support future warfighter needs could be adversely impacted by not having a geographically dispersed back-up capability and challenges in hiring and retaining qualified personnel to operate and maintain the system. Addressing these strategic planning and acquisition management challenges will help DOD sustain the progress it has made toward establishing enduring deployable biometric and forensic capabilities.

Recommendations for Executive Action

To enhance enterprise-wide biometric strategic planning, we recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics take the following two actions:

1. Publish an updated biometric strategic plan to identify enterprise goals and objectives; and
2. Publish a supporting biometric implementation plan that includes intended outcomes, measures of effectiveness, and responsibilities, among other things.

To facilitate more effective and efficient acquisition management of DOD's biometric and forensic enterprises, we recommend that the Secretary of the Army, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics take the following four actions:

3. Assign a milestone decision authority to oversee the Near Real Time Identity Operations solution;
4. Complete a disposition analysis for the Near Real Time Identity Operations solution before the solution reaches operation and sustainment;

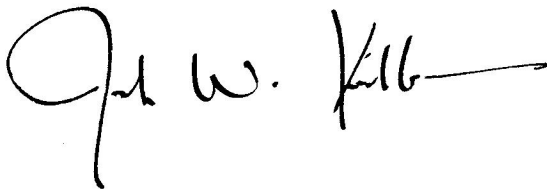
-
5. Consider including geographic dispersal as part of the selection criteria for the DOD ABIS follow-on system; and
 6. Use tradeoff selection criteria, rather than lowest-price technically acceptable criteria, for determining contractor support for DOD ABIS mission-critical functions when it is practicable to do so.

Agency Comments and Our Evaluation

DOD reviewed a draft of this report and concurred with all of our recommendations. DOD also cited actions it plans to take to address them. We believe that if DOD completes the actions it outlines in its response, this will address the intent of our recommendations. DOD's written comments are reprinted in their entirety in appendix V.

We are sending copies of this report to the appropriate congressional committees; the Secretary of Defense; the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Chairman, Joint Chiefs of Staff; the Secretaries of the Army, the Navy, and the Air Force; and the Commandant of the Marine Corps. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>

If you or your staff have any questions about this report, please contact me at (202) 512-9971 or at kirschbaumj@gao.gov. Key contributors to this report are listed in appendix VI.

A handwritten signature in black ink, appearing to read "Joe W. Kirschbaum", with a long horizontal stroke extending to the right.

Joseph W. Kirschbaum
Director, Defense Capabilities and Management

Appendix I: Objectives, Scope, and Methodology

This report evaluates the extent to which the Department of Defense (DOD) has since 2011 (1) validated enduring requirements for deployable biometric and forensic capabilities; (2) taken actions to meet enduring requirements for deployable biometric and forensic capabilities and overcome any related challenges; and (3) taken actions to address prior GAO recommendations regarding DOD's biometric and forensic capabilities. We did not assess digital; multimedia; cyber; or chemical, biological, radiological, and nuclear forensic requirements and capabilities.¹

To evaluate the extent to which DOD has validated enduring requirements for deployable biometric and forensic capabilities since 2011, we identified and analyzed non-materiel requirements documents drafted by the Army, as DOD's executive agent for biometrics and forensics, and validated by the Joint Requirements Oversight Council; and compared them to DOD's requirements validation process. We met with officials from the Defense Forensics and Biometrics Agency (DFBA) and the Army's Training and Doctrine Command to obtain greater specificity on the objective of each non-materiel requirement. We also identified biometric and forensic materiel requirements by analyzing relevant Office of the Secretary of Defense, military service, and combatant command strategies, plans, acquisition and sustainment documents, as well as written responses to question sets provided to each of the geographic combatant commands through the Joint Staff. This included reviewing and assessing the Army's 2015 analysis of alternatives and 2016 draft capability production document for DOD's authoritative biometric database to identify key performance requirements for the department's follow-on biometric database. We discussed the materiel biometric and forensic requirements with Joint Staff, military service, combatant command, and DFBA officials responsible for

¹ The Air Force and Defense Intelligence Agency have biometric and forensic responsibilities outside the scope of this review. Specifically, the Secretary of the Air Force is DOD's designated executive agent for digital and multimedia forensics, and the Director of the Defense Intelligence Agency is DOD's intelligence lead for biometric and forensic intelligence activities. We did not include intelligence agencies as part of this review

requirements planning and oversight to understand the requirements validation process for materiel solutions. We also met with geographic combatant command officials and analyzed the commands' written responses to a questionnaire to better understand their current and anticipated demand for biometric and forensic capabilities.

To evaluate the extent to which DOD has taken actions to meet enduring requirements for deployable biometric and forensic capabilities since 2011, we reviewed and analyzed relevant planning, acquisition, and sustainment documents, including emergent and urgent operational needs statements, analyses of alternatives, and capability development documents, to identify any challenges and gaps in meeting validated joint requirements. During the course of our analysis, we determined that a DOD-reported completion status of 75 percent or more was reflective of the validated non-materiel requirement having made significant progress. We also compared the content and process for developing DOD's biometric and forensic strategic plans with Standards for Internal Controls in the Federal Government for control activities to determine their enterprise utility. In addition, we compared federal information systems guidance on contingency planning with acquisition planning and development documents for DOD's follow-on authoritative biometric database. Furthermore, we reviewed and compared contracting information for providing service contracts to DFBA's Biometrics Operations Division, which manages the authoritative biometric database, with contracting provisions in the National Defense Authorization Act for Fiscal Year 2017 discouraging the use of lowest-price technically acceptable selection criteria in certain types of procurements. Finally, we met with Office of the Secretary of Defense, Joint Staff, military service, Special Operations Command (SOCOM), geographic combatant command, and DFBA officials responsible for biometric and forensic activities to determine the status of DOD's deployable non-materiel and materiel biometric and forensic capabilities, current and anticipated funding sources for materiel solutions, and estimated timeframes for completion.

To evaluate the extent to which DOD has taken actions to address our prior recommendations regarding its biometric and forensic capabilities since 2011, we reviewed our internal recommendation tracking system for status updates. We also analyzed DOD directives, guidance, and plans that had been updated or released since 2011, and written responses to our question set from each of the geographic combatant commands to

determine whether the department had taken actions that met the intent of our recommendations.² Finally, we met with program management, planning, and acquisition officials from the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and the military services to gather information and clarification on additional steps the department had taken or planned to take to address our prior recommendations.

To address our three reporting objectives, we met with biometric and forensic acquisition, operations, planning, and programming officials from the DOD organizations identified in table 4. We also met with officials from the Center for Naval Analyses to discuss their body of work on DOD biometrics and forensics.

Table 4: Department of Defense (DOD) Organizations Contacted by GAO^a

Office of the Secretary of Defense
Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
Joint Rapid Acquisition Cell
Defense Forensics and Biometrics Office
Office of the Under Secretary of Defense for Policy
Office of the Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance
Office of the Deputy Assistant Secretary of Defense for Countering Weapons of Mass Destruction
DOD Office of the Director, Operational Test and Evaluation
Net-Centric, Space & Missile Defense Systems
The Joint Staff
Force Structure, Resources, and Assessment Directorate (J8)
U.S. Army
Headquarters Department of the Army Deputy Chief of Staff for Operations, Plans and Training (G3/5/7)
Adaptive Counter Improvised Explosive Device and Explosive Ordnance Disposal Solutions (G38)

²DOD has six geographic combatant commands: U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Northern Command, U.S. Pacific Command, and U.S. Southern Command.

**Appendix I: Objectives, Scope, and
Methodology**

Training and Doctrine Command
Capabilities Manager - Terrestrial and Identity, Fort Huachuca, Arizona
Office of the Provost Marshal General
Defense Forensics and Biometrics Agency
Defense Forensics Science Center, Gillem Enclave, Georgia
Army Contracting Command – New Jersey, Picatinny Arsenal, New Jersey
Assistant Secretary of the Army for Acquisition, Logistics, and Technology
Program Executive Office, Intelligence Electronic Warfare and Sensors
Project Management Office for Department of Defense Biometrics

Defense Intelligence Agency, Identity Intelligence Project Office

U.S. Navy

Deputy Under Secretary of the Navy (Policy),
Security Directorate
Security Enterprise Branch
Naval Sea Systems Command
Naval Surface Warfare Center, Dahlgren Division, Dahlgren, Virginia
Naval Surface Warfare Center, Indian Head Explosive Ordnance Disposal Technology Division
Expeditionary Exploitation Unit One, Indian Head, Maryland
Naval Criminal Investigative Service

U.S. Marine Corps

Headquarters, Plans, Policies, and Operations Division
Security Division
Identity Operations Section
Marine Corps Combat Development Command
Combat Development and Integration
Capabilities Development Directorate

U.S. Special Operations Command, MacDill Air Force Base, Florida
Identity Intelligence Operations Division (I2)

U.S. Africa Command, Stuttgart, Germany
Identity Intelligence Program (J2X)

U.S. Central Command, MacDill Air Force Base, Florida
Joint Security Office (CCJ3)
Science and Technology Office (CCJ8)

U.S. European Command, Stuttgart, Germany
Intelligence Engagement (J2)
Identity Intelligence Branch

U.S. Northern Command, Peterson Air Force Base, Colorado
Operations Directorate (J3)
Identity Activities Cell (J34)
Homeland Defense and Protection Division

**Appendix I: Objectives, Scope, and
Methodology**

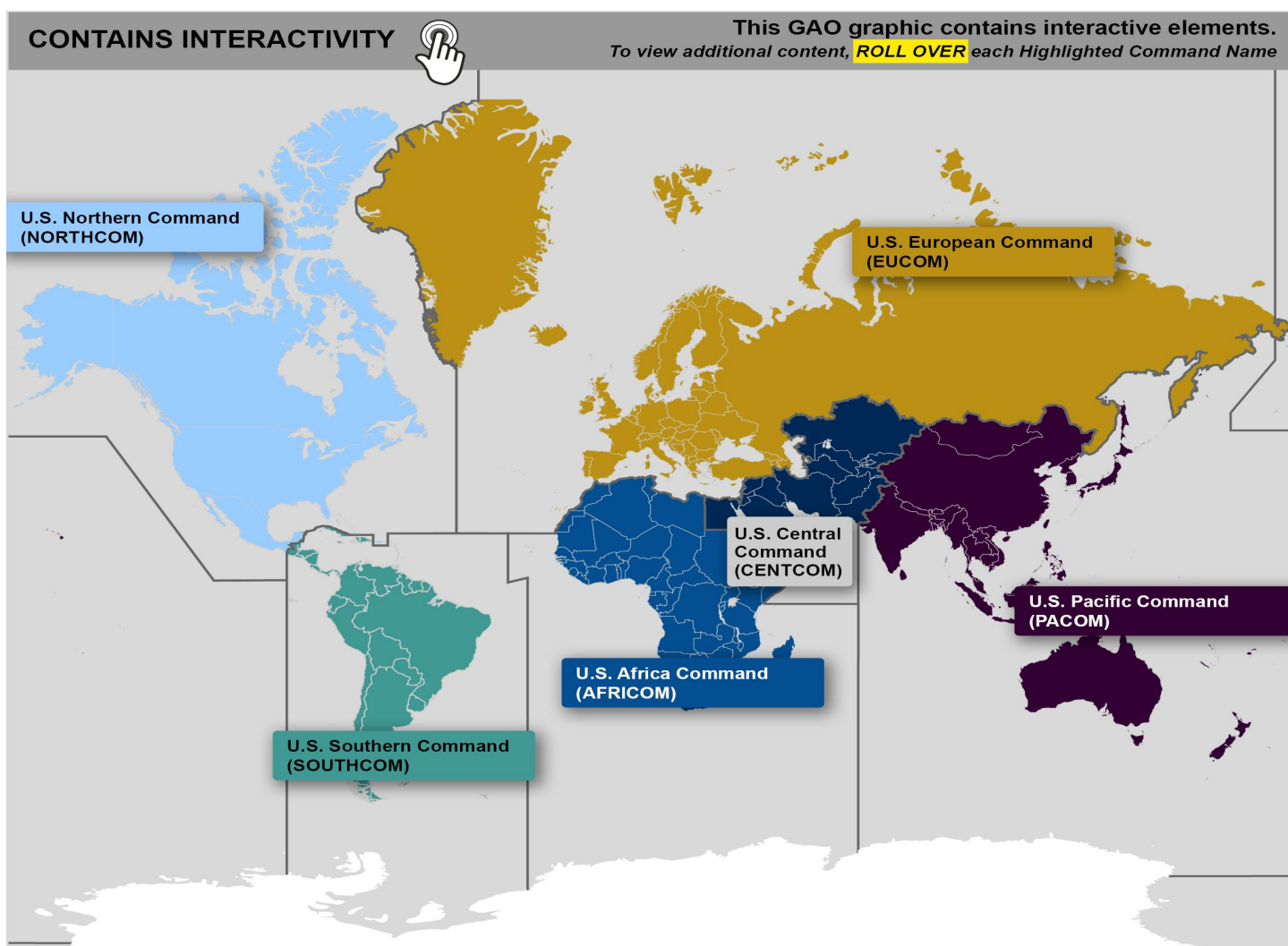
U.S. Pacific Command, Camp H.M. Smith, Hawaii
Anti-Terrorism Force Protection Office (J348)
Identity Operations

U.S. Southern Command, Miami, Florida
Identity Intelligence (I2)

Source: GAO. | GAO-17-580

^aUnless otherwise indicated, these organizations are located within the Washington, D.C., metropolitan area.

Appendix II: Geographic Combatant Commands' Demand for Biometric and Forensic Capabilities



Source: GAO analysis of Department of Defense information. | GAO-17-580

**Appendix II: Geographic Combatant
Commands' Demand for Biometric and
Forensic Capabilities**

Embedded data

U.S. Combatant Command	Demand Last 3-5 Years		Demand Next 3-5 Years	
	Biometrics	Forensics	Biometrics	Forensics
U.S. Africa Command	increased	increased	increased	increased
U.S. Central Command	increased	increased	increased	increased
U.S. European Command	increased	Stayed the same	decreased	decreased
U.S. Northern Command	increased	Not provided	increased	increased
U.S. Pacific Command	increased	increased	increased	increased
U.S. Southern Command	increased	increased	increased	increased

Appendix III: Department of Defense (DOD)-Validated, Non-materiel Enduring Biometric and Forensic Requirements

Between 2013 and 2014, DOD validated 30 non-materiel enduring requirements for its deployable biometric and forensic capabilities. These requirements are designed to transition DOD’s biometric and forensic capabilities, over a multi-year period, from rapidly acquired and OCO-funded capabilities to enduring capabilities resourced through base funding. The status and anticipated completion date of each requirement is detailed in table 5.

Table 5: Biometric and Forensic Non-materiel Enduring Requirement Status^a

Biometrics

Type	Requirement	Status	Department of Defense’s (DOD) Anticipated Completion Date
Doctrine	Integrate and broaden biometric and identity management tasks and processes into existing joint doctrine.	70 percent complete	August 2019
	Update and broaden biometric and/or identity management-related concepts and language into the joint operations family of concepts.	25 percent complete	August 2019
	Integrate biometric tasks into Joint Staff and combatant command plans and orders, where appropriate.	60 percent complete	August 2019
	Develop a biometric multi-service tactics, techniques, and procedures manual.	100 percent complete	May 2016
	Develop a stand-alone joint publication for identity operations that will include a discussion of biometrics and other capabilities supporting identity activities.	100 percent complete	August 2016
	Integrate biometrics into the Joint Lessons Learned Program process.	25 percent complete	August 2015

**Appendix III: Department of Defense (DOD)-
Validated, Non-materiel Enduring Biometric
and Forensic Requirements**

Type	Requirement	Status	Department of Defense's (DOD) Anticipated Completion Date
Organization	Establish a joint working group made up of representatives from the combatant commands and the military services to recommend a generic force structure to manage and provide biometrics.	35 percent complete	August 2019
Training	Integrate biometrics into the non-authoritative portions of the tasks within the universal joint task list.	75 percent complete	August 2019
	Make recommendations to Department of Defense (DOD) organizations for integrating biometrics into training.	25 percent complete	August 2019
	(Leadership and Education) Integrate tenets of biometrics into professional military education.	75 percent complete	August 2015
Policy	Revise the DOD directive on biometrics to account for expansion of the biometric enterprise.	100 percent complete	August 2015
	Make recommendation to develop an umbrella policy for DOD identity operations.	not started	August 2017
	Develop and publish a DOD instruction on biometrics.	0 - 50 percent complete	November 2018
	Develop and publish a DOD manual on the department's authoritative biometric database operations.	0 - 50 percent complete	August 2018
	Develop and publish a DOD manual establishing minimum security classification standards for biometrics.	100 percent complete	August 2015

Forensics

Type	Requirement	Status	Department of Defense's (DOD) Anticipated Completion Date
Doctrine	Integrate and broaden appropriate forensic language, functions, information development, forensic-enabled intelligence, evidence, and chain of custody requirements into existing joint doctrine.	25 percent complete	November 2020
	Update joint doctrine to include guidance for planning and coordinating forensic capabilities.	25 percent complete	November 2020
	In coordination with the services and Special Operations Command, develop a multi-service tactics, techniques, and procedures manual covering forensic activities that includes training and cooperative operations with host and partner nations.	50 percent complete	November 2020
Organization	Institutionalize current deployable, tailorable, scalable, and customizable forensic collection and analysis capabilities that satisfy joint force information requirements.	60 percent complete	November 2020
	Complete a review and an assessment of directed forensic collection, processing, exploitation, and dissemination capabilities, training, and task organization within DOD for potential institutionalizing.	60 percent complete	November 2020

**Appendix III: Department of Defense (DOD)-
Validated, Non-materiel Enduring Biometric
and Forensic Requirements**

Type	Requirement	Status	Department of Defense's (DOD) Anticipated Completion Date
Training	Integrate forensic functions into the non-authoritative portions of the tasks within the universal joint task list.	65 percent complete	November 2017
	Review existing training courses for forensic applicability. Review and integrate suitable forensic collection and analysis capabilities into appropriate and relevant training courses.	60 percent complete	November 2017
	Develop joint guidance that establishes a minimum training standard for forensic capabilities.	50 - 75 percent complete	November 2017
	Integrate forensics into the joint mission-essential task list and the agency mission-essential task list.	20 percent complete	November 2017
	(Leadership and Education) Develop a training strategy to integrate forensics into appropriate joint leadership and education.	10 percent complete	November 2016
Policy	(Personnel) Develop requirements for training, certifications, and accreditations for all levels of forensic collectors, examiners, and custodians to ensure that qualified personnel are available in all phases of joint operations.	70 percent complete	November 2016
	Recommend that the Defense Intelligence Agency develop and publish a forensic security classification guideline.	90 percent complete	November 2018
	Develop and publish policy for use cases for deoxyribonucleic acid (DNA) collection, analysis, storing, and sharing, when the collection does not clearly support law enforcement, medical, personnel accounting, or Title 50 intelligence purposes.	0 - 50 percent complete	November 2018
	Issue technical guidance on defense forensics authoritative database operations per DOD guidance.	20 percent complete	November 2018
	Develop a lexicon to standardize forensic vocabulary and taxonomy used to auto-populate database fields across the joint force.	50 percent complete	November 2018

Source: GAO analysis of Defense Forensics and Biometrics Agency documentation. (Sept. 1, 2016) | GAO-17-580.

*Status information was provided by the Defense Forensics and Biometrics Agency. GAO discussed and confirmed the accuracy of this information with Joint Staff, Army Training and Doctrine Command, and Defense Forensics and Biometrics Agency officials.

Appendix IV: Additional Actions Taken by Department of Defense (DOD) on Previously Closed GAO Recommendations

As of May 2017, DOD had implemented 15 of 16 recommendations from our prior reports. Table 6 summarizes the 15 closed recommendations and additional steps that DOD has taken since they were closed.

Table 6: Additional Department of Defense (DOD) Actions Taken on Previously Closed Biometric and Forensic Recommendations

Theme: DOD Conformance with Biometric Standards		
1	Recommendation: DOD should implement a process for updating collection devices to adopted standards to help ensure that all DOD systems related to biometrics, including collection devices, conform to adopted standards. (GAO-11-276)	
	Closed as Implemented: August 2015	Additional Actions Taken: In January 2016 the department published DOD Directive 8521.01E, <i>DOD Biometrics</i> , which assigns responsibilities to ensure that DOD biometric-related systems conform to adopted standards, such as requiring the Secretary of the Army to lead standards development for joint, common, and interagency biometric capabilities. Navy officials noted that they have taken a number of steps to ensure collection device conformance, such as working with the Joint Interoperability Test Command to obtain conformance certification on electronic biometric transmission specification version 1.2 for its Identity Dominance System. Marine Corps officials raised concerns that DOD's Biometric Automated Toolset—the program of record for the Army's biometric collection device—does not meet conformance standards; however, an Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) memorandum grants an exception to policy for the Toolset until 2019, when the Army is scheduled to replace the device.
2	Recommendation: DOD should implement a process for testing collection devices at a sufficiently detailed level to help ensure that all DOD systems related to biometrics, including collection devices, conform to adopted standards. (GAO-11-276)	
	Closed as Implemented: August 2015	Additional Actions Taken: In January 2016 the department published DOD Directive 8521.01E, <i>DOD Biometrics</i> , which assigns responsibilities to ensure that DOD biometric-related systems conform to adopted standards, such as requiring the Secretary of the Army to lead standards development for joint, common, and interagency biometric capabilities. Marine Corps officials noted that there is no Army-led conformance testing process, and instead the military services independently ensure that their systems are tested and the results are provided to the Defense Forensics and Biometrics Agency. For example, Navy officials responded that they have taken a number of steps to ensure conformance and compliance with standards, including obtaining DOD electronic biometric transmission specification version 1.2 conformance certification for its Identity Dominance System from the Joint Interoperability Test Command in November 2015. The Navy is working with the Army to test biometric collection device options for the Naval Criminal Investigative Service.

**Appendix IV: Additional Actions Taken by
Department of Defense (DOD) on Previously
Closed GAO Recommendations**

- 3 Recommendation: DOD should more fully define and further clarify the roles and responsibilities needed to achieve DOD's biometric program and objectives for all stakeholders that include ensuring collection devices conform to adopted standards. ([GAO-11-276](#))

Closed as Implemented: September 2015	Additional Actions Taken: In January 2016 the department published DOD Directive 8521.01E, <i>DOD Biometrics</i> , which assigns responsibilities to ensure that DOD biometric-related systems conform to adopted standards, such as requiring the Secretary of the Army to lead standards development for joint, common, and interagency biometric capabilities.
---------------------------------------	---

Theme: DOD Biometric Information-sharing Agreement

- 4 Recommendation: DOD should complete the memorandum of agreement with the Department of Homeland Security regarding the sharing of biometric information as appropriate and consistent with U.S. laws and regulations and international agreements, as well as information-sharing environment efforts. ([GAO-11-276](#))

Closed as Implemented: March 2011	Additional Actions Taken: In January 2016 the Assistant Secretary of Defense for Homeland Defense and Global Security, in coordination with the Department of Homeland Security, updated a 2011 memorandum of agreement to further improve information-sharing between the departments for biometric, biographic, and identity-management data for screening and identity-verification purposes.
-----------------------------------	--

Theme: DOD's Long-term Biometric System Capability Needs

- 5 Recommendation: DOD should identify its long-term biometric system capability needs, including the technological capacity and associated costs needed both to support the warfighter and to facilitate sharing of biometric information across federal agencies, and take steps to meet those capability needs, as appropriate and consistent with U.S. laws and regulations, international agreements, and available resources. ([GAO-11-276](#))

Closed as Implemented: August 2015	Additional Actions Taken: DOD continues to identify its long-term biometric system capability needs. For example, the Army has completed an analysis of alternatives for the Biometrics Enabling Capability, and selection of the replacement system for DOD's current Automated Biometric Identification System is scheduled for 2022. In addition, the Army has initiated an analysis of alternatives to identify the replacement biometric collection device for the Biometric Automated Toolset.
------------------------------------	--

Theme: DOD Biometric Lessons Learned Dissemination

- 6 Recommendation: DOD should assess the value of disseminating biometrics lessons learned from existing military service and combatant command lessons learned systems across DOD to inform relevant policies and practices. ([GAO-12-442](#))

Closed as Implemented: July 2013	Additional Actions Taken: None.
----------------------------------	---------------------------------

- 7 Recommendation: DOD should implement a lessons learned dissemination process as appropriate. ([GAO-12-442](#))

Closed as Implemented: July 2013	Additional Actions Taken: Navy officials noted that the Navy command that conducts explosive ordnance disposal activities recently revised its after-action reporting process to leverage the Joint Lessons Learned Information System. A portal was created for documenting and sharing biometric and forensic lessons learned that were gathered during deployments and exercises.
----------------------------------	--

Theme: DOD Biometrics Training For Leaders

- 8 Recommendation: DOD should expand biometrics training for leaders, to include the effective use of biometrics in combat operations. ([GAO-12-442](#))

**Appendix IV: Additional Actions Taken by
Department of Defense (DOD) on Previously
Closed GAO Recommendations**

	Closed as Implemented: February 2017	Actions Taken During This Review : Between February 2015 and January 2017, DOD included 25 biometric- and forensic-related tasks on its universal joint task list, which serves as the foundation for joint operations planning and is a prerequisite for developing training and education, among other things. These tasks include identifying threat networks, coordinating and collecting biometric material, and conducting site exploitation. DOD also issued a number of policy and guidance documents in 2016 that address biometric training, including a DOD directive; multi-service tactics, techniques, and procedures; and a joint doctrine note. Biometrics has been incorporated into training courses offered at the Army War College, the National Intelligence University, the Defense Intelligence Agency Academy, and the Federal Law Enforcement Training Center.
9	Recommendation: DOD should expand biometrics training for leaders, to include the importance of selecting appropriate candidates for training. (GAO-12-442)	
	Closed as Implemented: February 2017	Actions Taken During This Review : Between February 2015 and January 2017, DOD included 25 biometric- and forensic-related tasks on its universal joint task list, which serves as the foundation for joint operations planning and is a prerequisite for developing training and education, among other things. These tasks include identifying threat networks, coordinating and collecting biometric material, and conducting site exploitation. DOD also issued a number of policy and guidance documents in 2016 that address biometric training, including a DOD directive; multi-service tactics, techniques, and procedures; and a joint doctrine note. Biometrics has been incorporated into training courses offered at the Army War College, the National Intelligence University, the Defense Intelligence Agency Academy, and the Federal Law Enforcement Training Center.
10	Recommendation: DOD should expand biometrics training for leaders, to include the importance of tracking who has completed biometrics training prior to deployment, to help ensure appropriate assignments of biometrics collection responsibilities. (GAO-12-442)	
	Closed as Implemented: February 2017	Actions Taken During This Review : Between February 2015 and January 2017 DOD included 25 biometric- and forensic-related tasks on its universal joint task list, which serves as the foundation for joint operations planning and is a prerequisite for developing training and education, among other things. These tasks include identifying threat networks, coordinating and collecting biometric material, and conducting site exploitation. DOD also issued a number of policy and guidance documents in 2016 that address biometric training, including a DOD directive; multi-service tactics, techniques, and procedures; and a joint doctrine note. Biometrics has been incorporated into training courses offered at the Army War College, the National Intelligence University, the Defense Intelligence Agency Academy, and the Federal Law Enforcement Training Center.
Theme: DOD Biometrics Data Transmission		
11	Recommendation: DOD should identify and assign responsibility for biometrics data throughout the transmission process, regardless of the pathway the data travel, to include the time period between when warfighters submit their data from the biometrics collection device until the biometrics data reach DOD's Automated Biometric Identification System. (GAO-12-442)	
	Closed as Implemented: April 2017	Actions Taken During This Review : In December 2013 Congress reinforced our recommendation in the National Defense Authorization Act for Fiscal Year 2014, directing DOD to brief Congress on the most appropriate element to take responsibility for defining and managing the end-to-end performance of the biometric enterprise, beginning and ending at the point of biometric encounter. ^a In response, in September 2014 DOD provided a briefing to Congress that identified the Defense Forensics and Biometrics Agency as responsible for managing the end-to-end performance of the biometric enterprise, given its defense biometrics executive agent authorities. In January 2016 DOD updated its directive on defense biometrics, which highlighted that the DOD biometrics enterprise provides a critical end-to-end capability to support decision-making across the full range of military operations, and further assigned the Secretary of the Army with responsibility for leading and executing activities for the DOD biometrics enterprise.
Theme: DOD Forensic Strategic Plan		
12	Recommendation: DOD should incorporate key elements in its forensic strategic plan, implementation plans, and other associated guidance that are currently absent, including approaches for achieving goals and objectives, milestones and metrics to gauge the department's progress, and resources needed to meet its goals and objectives. (GAO-13-447)	

**Appendix IV: Additional Actions Taken by
Department of Defense (DOD) on Previously
Closed GAO Recommendations**

	Closed as Implemented: January 2017	Actions Taken During This Review : DOD issued its defense forensic enterprise strategy in March 2015 and a follow-on implementation plan in September 2015. Between these two publications, milestones and metrics were identified and offices of primary responsibility were assigned with, among other things, identifying the necessary resources to accomplish the stated goals and objectives. Navy officials said that they have worked to address the goals and objectives by sustaining current forensic capabilities in three combatant commands and developing a Navy enlisted classification code—Explosive Ordnance Disposal Exploitation Specialist—for qualified personnel who receive training in the exploitation and analysis of forensic and biometric materials, among other things.
13	Recommendation: DOD should set a date to publish the strategic plan for the Defense Forensic Enterprise. (GAO-13-447)	
	Closed as Implemented: January 2017	Actions Taken During This Review : In March 2015 DOD published its defense forensic enterprise strategic plan.
Theme: Military Services' and Special Operations Command's Forensic Budget Estimates		
14	Recommendation: DOD should periodically review and evaluate the military services' and Special Operations Command's proposed forensic budget estimates—including expeditionary forensics—to help ensure that the department's overarching requirements and objectives will be met, in accordance with the DOD Defense Forensic Enterprise directive. (GAO-13-447)	
	Closed as Implemented: January 2017	Actions Taken During This Review : The Defense Forensics and Biometrics Office within the Office of the USD(AT&L) conducted a review from July 2014 to January 2015 on the military services' and Special Operations Command's forensic budget estimate submissions and requirements covering fiscal years 2015 through 2020. The Defense Biometrics and Forensics Office determined that current and proposed forensic budget estimates were adequate.
15	Recommendation: DOD should issue guidance on how the military services and Special Operations Command are to collect and report their forensic budget data—including expeditionary forensic budget data. (GAO-13-447)	
	Closed as Implemented: January 2017	Actions Taken During This Review : The Defense Biometrics and Forensics Office within the Office of the USD(AT&L) issued joint guidance in 2015 directing the use of DOD's planning, programming, budgeting, and execution process to determine the adequacy of the military services' and Special Operations Command's funding against validated forensics requirements.

Source: GAO analysis of DOD information. | GAO-17-580

^aNational Defense Authorization Act for Fiscal Year 2014, Pub.L. No. 113-66, div. A, title II, subtitle E, § 265 (Dec. 26, 2013).

Appendix V: Comments from the Department of Defense



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

JUL 14 2017

Mr. Joseph Kirschbaum
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Kirschbaum:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-17-580SU, "DOD BIOMETRICS AND FORENSICS: Progress Made in Establishing Long-term Deployable Biometric and Forensic Capabilities, but Further Actions Are Needed" dated May 31, 2017 (GAO Code 100914).

The Department is pleased with the report's finding that DoD has made significant progress in addressing its long-term requirements for deployable biometric and forensic capabilities. This progress is the result of many years of hard work by the men and women in multiple organizations across the Services, Joint Staff, Combatant Commands, and Office of the Secretary of Defense.

The Department recognizes that biometric and forensic capabilities have proven effective in identifying our adversaries and will remain an integral part of our future global force. The Department is committed to ensuring it maintains sufficient capabilities to support the national defense strategy and the needs of the Combatant Commands.

My point of contact is Mr. Ken Kroupa who can be reached at 703-697-4077 and kenneth.j.kroupa.civ@mail.mil.

Sincerely,

A handwritten signature in blue ink, appearing to read "Mary J. Miller".

Mary J. Miller
Acting

GAO Draft Report Dated May 31, 2017
GAO-17-580SU (GAO CODE 100914)

**“DOD BIOMETRICS AND FORENSICS: PROGRESS MADE IN ESTABLISHING
LONG-TERM DEPLOYABLE BIOMETRIC AND FORENSIC CAPABILITIES, BUT
FURTHER ACTIONS ARE NEEDED”**

**DEPARTMENT OF DEFENSE RESPONSE
TO THE GAO RECOMMENDATION**

RECOMMENDATION 1: To enhance enterprise-wide biometric strategic planning, GAO recommends that the USD(AT&L) publish an updated biometric strategic plan to identify enterprise goals and objectives.

DoD RESPONSE: Concur. The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics plans to publish an updated biometric strategic plan that identifies the goals and objectives of the Enterprise by December 2018.

RECOMMENDATION 2: To enhance enterprise-wide biometric strategic planning, GAO recommends that the USD(AT&L) publish a supporting biometric implementation plan that includes intended outcomes, measures of effectiveness, and responsibilities, among other things.

DoD RESPONSE: Concur. Upon approval of the updated biometric strategic plan, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics plans to publish a biometric implementation plan by December 2019. The implementation plan will identify tasks, outcomes, measures of effectiveness and assign responsibility for execution.

RECOMMENDATION 3: To facilitate more effective and efficient acquisition management of DOD’s biometric and forensic enterprises, GAO recommends that the Secretary of the Army, in coordination with the USD(AT&L), assign a milestone decision authority to oversee the Near Real Time Identity Operations solution.

DoD RESPONSE: Concur. By August 2017, Program Executive Office, Intelligence, Electronic Warfare and Sensors (PEO IEW&S) will conduct an assessment of the Near Real Time Identity Operations solution and develop a plan to transition Milestone Decision Authority to the Office of Primary Responsibility. The PEO IEW&S will brief the plan to the Army Acquisition Executive by fourth quarter, fiscal year 2017.

RECOMMENDATION 4: To facilitate more effective and efficient acquisition management of DOD's biometric and forensic enterprises, GAO recommends that the Secretary of the Army, in coordination with the USD(AT&L), complete a disposition analysis for the Near Real Time Identity Operations solution before the solution reaches operation and sustainment.

DoD RESPONSE: Concur. By fourth quarter fiscal year 2017, Program Executive Office, Intelligence, Electronic Warfare and Sensors will provide the Army Acquisition Executive their recommendations for cost, schedule, and performance parameters to provide the Near Real Time Identity Operations capability in the most effective and efficient manner and to inform a disposition analysis that will be conducted before the solution reaches operation and sustainment.

RECOMMENDATION 5: To facilitate more effective and efficient acquisition management of DOD's biometric and forensic enterprises, GAO recommends that the Secretary of the Army, in coordination with the USD(AT&L), consider including geographic dispersal as part of the selection criteria for the DOD ABIS follow-on system.

DoD RESPONSE: Concur. Program Executive Office, Intelligence, Electronic Warfare and Sensors will conduct a cost-benefit-risk trade-off assessment to geographically disperse the DoD Automated Biometric Identification System (ABIS) follow-on system. The outcome of this assessment will be considered in 2019 as part of the overall system architecture determination for the DoD ABIS follow on capability.

RECOMMENDATION 6: To facilitate more effective and efficient acquisition management of DOD's biometric and forensic enterprises, GAO recommends that the Secretary of the Army, in coordination with the USD(AT&L), use tradeoff selection criteria, rather than lowest price technically acceptable criteria, for determining contractor support for DOD ABIS mission-critical functions when it is practicable to do so.

DoD RESPONSE: Concur. The Army Contracting Command is working to award the knowledge based DoD ABIS support service contracts on a best value tradeoff basis. The current contracts end in November 2017.

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Joseph W. Kirschbaum, (202) 512-9971 or kirschbaumj@gao.gov

Staff Acknowledgments

In addition to the contact above, Marc Schwartz, Assistant Director; David Adams; Vincent Buquicchio; Pamela Davidson; Richard Hung; Amber Lopez Roberts; Paul Seely; Sarah Warmbein; and Cheryl Weissman made key contributions to this report.

Appendix VII: Accessible Data

Agency Comment Letter

Accessible Text for Appendix V: Comments from the
Department of Defense

Page 1

ASSISTANT SECRETARY OF DEFENSE

3030 DEFENSE PENTAGON

WASHINGTON, DC 20301-3030

AND ENGINEERING

JUL 14 2017

Mr. Joseph Kirschbaum

Director, Defense Capabilities and Management

U.S. Government Accountability Office

441 G Street, N.W.

Washington, DC 20548

Dear Mr. Kirschbaum:

This is the Department of Defense (DoD) response to the Government
Accountability Office (GAO) Draft Report, GAO-17-580SU, "DOD
BIOMETRICS AND FORENSICS:

Progress Made in Establishing Long-term Deployable Biometric and Forensic Capabilities, but Further Actions Are Needed" dated May 31, 2017 (GAO Code 100914).

The Department is pleased with the report's finding that DoD has made significant progress in addressing its long-term requirements for deployable biometric and forensic capabilities. This progress is the result of many years of hard work by the men and women in multiple organizations across the Services, Joint Staff, Combatant Commands, and Office of the Secretary of Defense.

The Department recognizes that biometric and forensic capabilities have proven effective in identifying our adversaries and will remain an integral part of our future global force. The Department is committed to ensuring it maintains sufficient capabilities to support the national defense strategy and the needs of the Combatant Commands.

My point of contact is Mr. Ken Kroupa who can be reached at 703-697-4077 and kenneth.j.kroupa.civ@mail.mil.

Page 2

GAO Draft Report Dated May 31, 2017 GA0-17-580SU (GAO CODE 100914)

"DOD BIOMETRICS AND FORENSICS: PROGRESS MADE IN ESTABLISHING LONG-TERM DEPLOYABLE BIOMETRIC AND FORENSIC CAPABILITIES, BUT FURTHER ACTIONS ARE NEEDED"

DEPARTMENT OF DEFENSE RESPONSE TO THE GAO RECOMMENDATION

RECOMMENDATION 1: To enhance enterprise-wide biometric strategic planning, GAO recommends that the USD(AT&L) publish an updated biometric strategic plan to identify enterprise goals and objectives.

DoD RESPONSE: Concur. The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics plans to publish an updated biometric strategic plan that identifies the goals and objectives of the Enterprise by December 2018.

RECOMMENDATION 2: To enhance enterprise-wide biometric strategic planning, GAO recommends that the USD(AT&L) publish a supporting biometric implementation plan that includes intended outcomes, measures of effectiveness, and responsibilities, among other things.

DoD RESPONSE: Concur. Upon approval of the updated biometric strategic plan, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics plans to publish a biometric implementation plan by December 2019. The implementation plan will identify tasks, outcomes, measures of effectiveness and assign responsibility for execution.

RECOMMENDATION 3: To facilitate more effective and efficient acquisition management of DOD's biometric and forensic enterprises, GAO recommends that the Secretary of the Army, in coordination with the USD(AT&L), assign a milestone decision authority to oversee the Near Real Time Identity Operations solution.

DoD RESPONSE: Concur. By August 2017, Program Executive Office, Intelligence, Electronic Warfare and Sensors (PEO IEW&S) will conduct an assessment of the Near Real Time Identity Operations solution and develop a plan to transition Milestone Decision Authority to the Office of Primary Responsibility. The PEO IEW&S will brief the plan to the Army Acquisition Executive by fourth quarter, fiscal year 2017.

Page 3

RECOMMENDATION 4: To facilitate more effective and efficient acquisition management of DOD's biometric and forensic enterprises, GAO recommends that the Secretary of the Army, in coordination with the USD(AT&L), complete a disposition analysis for the Near Real Time Identity Operations solution before the solution reaches operation and sustainment.

DoD RESPONSE: Concur. By fourth quarter fiscal year 2017, Program Executive Office, Intelligence, Electronic Warfare and Sensors will provide the Army Acquisition Executive their recommendations for cost, schedule, and performance parameters to provide the Near Real Time Identity Operations capability in the most effective and efficient manner and to inform a disposition analysis that will be conducted before the solution reaches operation and sustainment.

RECOMMENDATION 5: To facilitate more effective and efficient acquisition management of DOD's biometric and forensic enterprises, GAO recommends that the Secretary of the Army, in coordination with the USD(AT&L), consider including geographic dispersal as part of the selection criteria for the DOD ABIS follow-on system.

DoD RESPONSE: Concur. Program Executive Office, Intelligence, Electronic Warfare and Sensors will conduct a cost-benefit-risk trade-off assessment to geographically disperse the DoD Automated Biometric Identification System (ABIS) follow-on system. The outcome of this assessment will be considered in 2019 as part of the overall system architecture determination for the DoD ABIS follow on capability.

RECOMMENDATION 6: To facilitate more effective and efficient acquisition management of DOD's biometric and forensic enterprises, GAO recommends that the Secretary of the Army, in coordination with the USD(AT&L), use tradeoff selection criteria, rather than lowest price technically acceptable criteria, for determining contractor support for DOD ABIS mission-critical functions when it is practicable to do so.

DoD RESPONSE: Concur. The Army Contracting Command is working to award the knowledge based DoD ABIS support service contracts on a best value tradeoff basis. The current contracts end in November 2017.