



Department of Defense **DIRECTIVE**

NUMBER 8521.01E

January 13, 2016

Incorporating Change 2, Effective October 15, 2018

USD(R&E)

SUBJECT: DoD Biometrics

References: See Enclosure 1

1. PURPOSE. This directive:

a. Reissues DoD Directive (DoDD) 8521.01E (Reference (a)) to establish policy and assign responsibilities for DoD biometrics.

b. Designates the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) as the Biometrics Principal Staff Assistant (PSA) responsible for oversight of DoD biometric activities and policy.

c. Designates the Secretary of the Army as the DoD Executive Agent (EA) for Biometrics in accordance with Public Law 106-246 (Reference (b)) and DoDD 5101.1 (Reference (c)).

2. APPLICABILITY. This directive:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this directive as the "DoD Components").

b. Does not apply to physical evidence or other biometric material collected either pursuant to a criminal investigation or as directed by DoD Instruction 5505.14 (Reference (d)).

3. POLICY. It is DoD policy that:

a. The DoD Biometrics Enterprise provide a critical end-to-end capability through a defined operations or intelligence cycle to support tactical and operational decision-making across the full range of military operations for DoD warfighting, intelligence, law enforcement, security,

force protection, homeland defense, counterterrorism, business, and information environment mission areas (referred to in this directive as “DoD mission areas”).

b. DoD biometric programs be designed to improve the effectiveness and efficiency of identity activities and to eliminate unwarranted duplication of technology development and information management efforts.

c. Biometric collections are encouraged during all military operations and military intelligence activities where legal and appropriate.

d. The maintenance, collection, use, and dissemination of biometric data, which includes the transmission, storage, caching, tagging, analysis, production, and use of biometric data adhere to applicable laws, policies, standards, and protocols, including but not limited to DoDD 5400.11 (Reference (e)), to support data sharing and interoperability.

e. The DoD biometric and intelligence enterprises are to be integrated and interoperable through the use of identity intelligence capabilities, including biometric enabled intelligence (BEI), to the fullest extent possible to enable DoD and mission partners’ operations.

f. Biometric, biographic, behavioral, and contextual data collected and maintained by DoD Components, as well as resulting BEI products, are to be considered DoD data, protected from unauthorized release, and shared in accordance with applicable data sharing and disclosure policy under appropriate authorities, arrangements, and agreements. Foreign-collected identity information that is shared with the DoD is to be withheld from public disclosure to avoid the adverse effects such a release would have on the DoD’s ability to obtain the same or similar information in the future.

g. The DoD maintain authoritative biometric data repositories to conduct match, store, and share functions for the DoD mission areas of:

(1) Individuals whose biometric data were collected as a part of national security-related operations, including bulk collections from interagency or foreign partner repositories; or

(2) Individuals affiliated with or seeking to be affiliated with the DoD whose biometric data were obtained for a legitimate, authorized, and DoD purpose in accordance with applicable law, regulation, and policy.

h. Biometric, biographic, behavioral, and contextual data collected and maintained by DoD Components and BEI are to be unclassified or classified at the lowest appropriate level consistent with standard criteria for security classification and in accordance with applicable security classification guidance to support interagency and international data accessibility.

i. The DoD develop and maintain continuity of operations and disaster recovery plans for vital biometric capabilities.

j. The DoD make available to other U.S. Government agencies all biometric and associated biographic and contextual data collected during the course of military operations to support national security screening and vetting activities to the fullest extent permitted by law.

k. The DoD comply with National Security Presidential Directive-59/Homeland Security Presidential Directive (HSPD)-24 (Reference (f)) and the Biometrics for Identification and Screening to Enhance National Security Action Plan (Reference (g)).

4. RESPONSIBILITIES. See Enclosure 2.

5. INFORMATION COLLECTION REQUIREMENTS. The DoD Biometrics Enterprise Results, referred to in paragraph 11g of Enclosure 2, does not require licensing with a report control symbol in accordance with paragraph 1b(16) of Volume 1 of DoD Manual 8910.01 (Reference (h)).

6. RELEASABILITY. **Cleared for public release.** This directive is available on the Directives Division Website at <http://www.esd.whs.mil/DD/>.

7. SUMMARY OF CHANGE 2. This change reassigns the office of primary responsibility for this directive to the Under Secretary of Defense for Research and Engineering in accordance with the July 13, 2018 Deputy Secretary of Defense Memorandum (Reference (i)).

8. EFFECTIVE DATE. This directive is effective January 13, 2016.



Robert O. Work
Deputy Secretary of Defense

Enclosures

1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 8521.01E, "Department of Defense Biometrics," February 21, 2008 (hereby cancelled)
- (b) Section 112 of the Emergency Supplemental Act, 2000, Division B of Public Law 106-246, July 13, 2000
- (c) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002, as amended
- (d) DoD Instruction 5505.14, "Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations, Law Enforcement, Corrections, and Commanders," December 22, 2015, as amended
- (e) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
- (f) National Security Presidential Directive-59/Homeland Security Presidential Directive-24, "Biometrics for Identification and Screening to Enhance National Security," June 5, 2008
- (g) Office of the Attorney General of the United States, "Biometrics for Identification and Screening to Enhance National Security: Action Plan," November 2008¹
- (h) DoD Manual 8910.01, Volume 1, "DoD Information Collections: Procedures for DoD Internal Information Collections," June 30, 2014
- (i) Deputy Secretary of Defense Memorandum, "Establishment of the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment," July 13, 2018
- (j) DoD Directive 5530.3, "International Agreements," June 11, 1987, as amended
- (k) Title 10, United States Code
- (l) DoD Directive 5105.21, "Defense Intelligence Agency (DIA)," March 18, 2008
- (m) DoD Instruction O-3300.04, "Defense Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI)," May 25, 2012
- (n) DoD Instruction 1000.25, "DoD Personnel Identity Protection (PIP) Program," March 2, 2016
- (o) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
- (p) United States Army, "DoD Capstone Concept of Operations for Employing Biometrics in Military Operations," June 10, 2012
- (q) Joint Publication 2-0, "Joint Intelligence," current edition

¹ Available from the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security.

ENCLOSURE 2

RESPONSIBILITIES

1. USD(AT&L). In his or her capacity as the Biometrics PSA, the USD(AT&L):

a. Oversees and, as required, directs the activities of the DoD Biometrics Enterprise and the DoD EA for Biometrics, in accordance with Reference (c).

b. Facilitates the development and implementation of policy for DoD biometrics in coordination with the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense for Intelligence (USD(I)), and the DoD EA for Biometrics.

c. Serves as the primary DoD point of contact for other U.S. Government agencies and international entities on all biometric-related activities unless specified in this directive, DoD policy, or applicable law.

d. Appoints an official to chair the DoD Biometrics Executive Committee (EXCOM).

2. ASSISTANT SECRETARY OF DEFENSE FOR ACQUISITION. The Assistant Secretary of Defense for Acquisition manages the alignment and compliance of biometric-related acquisitions with DoD Biometrics Enterprise objectives and policies.

3. USD(P). The USD(P):

a. Develops and oversees the implementation of policy for DoD biometrics in coordination with the USD(AT&L), the USD(I), and the DoD EA for Biometrics.

b. Approves biometric sharing arrangements and agreements for areas under the authority of the USD(P), and as appropriate, coordinates these arrangements and agreements with other U.S. Government agencies and international entities in accordance with DoDD 5530.3 (Reference (j)).

c. Determines whether foreign-collected identity information is eligible for exemption in accordance with section 130c of Title 10, United States Code (Reference (k)) in coordination with the USD(I).

4. USD(I). The USD(I):

a. Oversees DoD Component BEI policy, activities, and programs that support identity activities for the DoD mission areas and the DoD Biometrics Enterprise.

b. Establishes standard criteria for security classification of certain biometric data and other biometric-related information.

c. Coordinates with the Biometrics PSA on intelligence, to include BEI programs, activities, and agreements that may affect biometric-related authorities and missions.

d. Oversees the integration of biometrics and BEI into the DoD intelligence, counterintelligence, and defense security enterprises in coordination with the Director of National Intelligence.

e. Serves as the primary point of contact for other U.S. Government agencies and international entities on all BEI-related activities.

5. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I), the Director, DIA:

a. Serves as the DoD intelligence lead for biometric activities and programs in accordance with DoDD 5105.21 (Reference (l)) and DoD Instruction O-3300.04 (Reference (m)).

b. Facilitates delivery of BEI capabilities within the intelligence process to support a defined operations or intelligence cycle in coordination with the DoD intelligence components and the DoD EA for Biometrics.

c. Coordinates and synchronizes development and implementation of DoD biometric collection strategies for the DoD mission areas.

d. Develops, maintains, manages, and shares a DoD biometric enabled watchlist.

6. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS. The Under Secretary of Defense for Personnel and Readiness:

a. Merges biometrics into the policies and procedures under his or her purview.

b. Oversees and maintains the DoD authoritative biometric data repository for match, store, and share functions for individuals affiliated or seeking to be affiliated with the DoD. This repository contains authoritative identity information for the issuance of identity credentials in accordance with DoDI 1000.25 (Reference (n)).

7. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE. The Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense maintains the visibility of biometric-related funding.

8. DEPUTY CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE. In his or her capacity as the DoD Privacy and Civil Liberties Officer, the Deputy Chief Management Officer of the Department of Defense:

a. Ensures that the maintenance, use, collection, and dissemination of biometric information are conducted in accordance with Reference (e) and that DoD biometric policies and procedures also comply with DoDD 5200.27 (Reference (o)).

b. Directs all privacy and civil liberties issues related to the maintenance, use, collection, and dissemination of biometric data be coordinated with the Directorate for Oversight and Compliance, Defense Privacy and Civil Liberties Division in the Office of the Deputy Chief Management Officer.

9. DOD COMPONENT HEADS, EXCEPT FOR THE CJCS. The DoD Component heads, except for the CJCS:

a. Designate a general or flag officer or Senior Executive Service-equivalent individual to serve as a member on the DoD Biometrics EXCOM.

b. Notify and coordinate all biometric and BEI activities and acquisitions with the Biometrics PSA, the Assistant Secretary of Defense for Acquisition, the USD(I), the DoD EA for Biometrics, and the Director, DIA.

c. Plan, program, budget for, and field DoD Component-required and, where appropriate, joint and common biometric and BEI capabilities and institutional training requirements to support identity activities in accordance with Reference (k) and Major Force Program-11 authorities.

d. Adhere to DoD-approved standards, protocols, and enterprise architectures.

10. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in section 9 of this enclosure, the Secretaries of the Military Departments ensure policy and guidance exist to maintain oversight of their Department's biometric and BEI capabilities.

11. SECRETARY OF THE ARMY. In addition to the responsibilities in sections 9 and 10 of this enclosure, and in his or her capacity as the DoD EA for Biometrics, the Secretary of the Army:

a. Appoints a general or flag officer or Senior Executive Service official to serve as the focal point of the DoD Biometrics Enterprise to plan, program, and budget sufficient resources to execute the responsibilities of the DoD EA for Biometrics in accordance with Reference (c) and this directive.

- b. Leads and executes common storage, matching, analysis, and sharing activities of the DoD Biometrics Enterprise for biometric data collected as a part of military operations.
- c. Requires DoD Components' biometric products, systems, and services to adhere to applicable standards, protocols, and the DoD biometric authoritative enterprise reference architecture to support interoperability.
- d. Leads requirements, architecture, and standards development for joint, common, and interagency biometric capabilities.
- e. Acquires common biometric capabilities to support the operational requirements of the joint force commander.
- f. Oversees and maintains the DoD's authoritative biometric data repository for match, store, and share functions for the DoD mission areas of individuals whose biometric data were collected as a part of operations and, subject to Reference (o) and/or the approval by the Deputy Chief Management Office, individuals not affiliated with or seeking to be affiliated with the DoD.
- g. Measures the health and performance of the DoD Biometrics Enterprise and generates results for the Biometrics PSA and the DoD Biometrics EXCOM.
- h. Exchanges biometric data with appropriate DoD, interagency, State, tribal, local, and international partners in accordance with applicable law, regulation, policy, and data sharing arrangements and agreements.
- i. Leads implementation of DoD military detainee national security threat activities, in coordination with the Director, DIA, and pursuant to Reference (g).
- j. Acts as the DoD point of contact for execution of biometric-related activities or as directed and assigned by the Biometrics PSA.
- k. Directs the execution of concluded biometric-related agreements with other U.S. Government agencies and international entities, and notifies the Biometrics PSA, the USD(P), and the USD(I) of the need for their initiation, modification, suspension, or cancellation.
- l. Appoints an official to serve as a co-chair of the DoD Biometrics EXCOM.

12. CJCS. The CJCS coordinates and monitors fulfillment of validated joint requirements for biometrics and BEI, and appoints an official to serve as a co-chair of the DoD Biometrics EXCOM.

13. COMBATANT COMMANDERS. In addition to the responsibilities in section 9 of this enclosure, the Combatant Commanders identify biometric and BEI capability and policy gaps that inhibit achievement of operational objectives; develop and issue guidance on the use of

biometrics and BEI within their areas of responsibility; and engage mission partners to employ biometric capabilities and share biometric data in support of identity activities in coordination with the USD(P), the USD(I), the Director, DIA, the CJCS, and the DoD EA for Biometrics.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

BEI	biometric enabled intelligence
CJCS	Chairman of the Joint Chiefs of Staff
DIA	Defense Intelligence Agency
DoDD	DoD directive
EA	Executive Agent
EXCOM	Executive Committee
HSPD	Homeland Security Presidential Directive
PSA	Principal Staff Assistant
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this directive.

BEI. Defined in Reference (m).

biometric enabled watchlist. Defined in Reference (m).

biometric data. Computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates, and/or similarity scores. Biometric data is used to describe the information collected during an enrollment, verification, or identification process but the term does not apply to end user information such as user name, demographic information, or authorizations.

biometrics. The process of recognizing an individual based on measurable anatomical, physiological, or behavioral characteristics.

collect. Defined in Capstone Concept of Operations for Employing Biometrics in Military Operations (Reference (p)).

contextual data. Defined in Reference (p).

DoD Biometrics Enterprise. An entity comprised of DoD joint, Service, and agency operations, intelligence, law enforcement, and security organizations working together to integrate biometrics into the identity transactions needed to support military operations, activities, and departmental business functions.

identity activities. A collection of functions and actions that appropriately recognize and characterize an entity from another entity to support decision making. Activities include the collection of identity attributes and captured materials, their processing and exploitation, all-source analytic efforts, and production and dissemination of identity intelligence products to inform policy and strategy development, operational planning and assessment, and appropriate action at the point of encounter.

identity intelligence. Defined in Joint Publication 2-0 (Reference (q)).

match. Defined in Reference (p).

military detainee national security threat. Defined in Reference (g).

share. Defined in Reference (p).

store. Defined in Reference (p).