A0025-2b DoD PMG (DFBA)

System name:
Defense Biometric Identification Records System

System location:
Department of Defense, Defense Forensics and Biometrics Agency, Biometrics Identity Management Activity, 347 West Main Street, Clarksburg, WV 26306-2947.

Any DoD location at which any DoD activity operates biometric data collection and/or storage systems (for which notice is not provided elsewhere) that receives, compares, retains, accesses, uses, or forwards biometric data and related information to or from the above-referenced database.

Categories of individuals covered by the system:
Individuals covered include members of the U.S. Armed Forces; DoD civilian and contractor personnel; military reserve personnel; Army and Air National Guard personnel; U.S. persons requiring or requesting access to DoD, DoD-controlled, and/or DoD contractor operated, controlled or secured data, information systems, equipment, facilities or installations.

DoD-affiliated U.S. persons who have been declared missing or prisoners of war; DoD-affiliated U.S. persons who are being detained or held hostage by hostile forces, or non-DoD affiliated U.S. persons known or suspected to be held under such circumstances in an area of DoD operations; U.S. persons recovered from hostile control by DoD personnel or as a result of DoD operations; U.S. persons within the purview of the DoD personnel recovery mission which supports U.S. military, DoD civilian, and DoD contractor personnel while hostilities are ongoing.

U.S. persons within the purview of the DoD personnel accounting mission which supports U.S. military, DoD civilian, and DoD contractor personnel once hostilities cease; U.S. persons in DoD custody as a result of military operations overseas or due to maritime intercepts; U.S. persons otherwise encountered by DoD forces during military operations.

U.S. Persons lawfully assessed by appropriate authority in accordance with applicable law and policy to pose a potential threat to DoD personnel, installations, assets, information and/or operations.

U.S. Persons who are the subject of pending queries against the subject record system.

U.S. persons identified during a biometric screening process as a possible identity match to the subject of an existing record within the system.

U.S. Persons who are misidentified as a possible identity match to the subject of an existing record within the system ("misidentified persons").

U.S. persons who are the subject of a redress inquiry that is pending resolution.

U.S. and non-U.S. persons whose biometrics are collected by federal, state, local, tribal, foreign, or international agencies for national security, law enforcement, immigration, intelligence, or other DoD mission-related functions, and who are determined to be subjects of interest to the DoD.

Categories of records in the system:
This system includes identity records established to support automated identification, authentication, or verification including biometric information and related biographic, contextual, and other information, reports, and data in paper and/or electronic format.

Records may include:

Biometric information including images, photos and templates of biological (anatomical and physiological) and/or behavioral characteristics that can be used for automated recognition, including, fingerprints, palm prints, facial images, iris images, DNA, and voice samples.

Biographic information including name, date of birth, place of birth, height, weight, eye color, hair color, race, gender, and similar relevant information;

Contextual information including organization, telephone number, office symbol, security clearance, level of access, and location of collection.

User Information including subject interest codes; user identification codes; globally unique identifiers; data files retained by users; assigned passwords; magnetic tape reel

identification; abstracts of computer programs and names and phone numbers of contributors, and similar relevant information;

Information concerning DoD-affiliated persons who are being detained or held hostage by hostile forces, or non-DoD affiliated U.S. persons known or suspected to be held under such circumstances in an area of DoD operations, such as biographic data, casualty reports, and debriefing reports;

Information from and electronic images of international federal, state, tribal, or state issued individual identity documents.

NOTE: This notice expressly does not pertain to any record or information maintained in any DoD system of records that is subject to Executive Order 12333, United States intelligence activities; DoDD 5240.01, DoD Intelligence Activities and/or Army Regulation 381-10, U.S. Army Intelligence Activities.

Authority for maintenance of the system:
10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Army; Homeland Security Presidential Directive (HSPD)-6, Integration and Use of Screening Information; HSPD-11, Comprehensive Terrorist-Related Screening Procedures; National Security Presidential Directive (NSPD)-59/HSPD-24, Biometrics for Identification and Screening to Enhance National Security; DoDI 2000.12, DoD Antiterrorism (AT) Program; DoD Instruction 2310.5, Accounting for Missing Persons; DoD Directive 2310.7, Personnel Accounting – Losses Due to Hostile Acts; Defense Prisoner of War/Missing in Action Office; DoDI 5200.08, Security of DoD Installations and Resources; DoDD 8521.01E, DoD Biometrics; DoDD 8500.1, Information Assurance; DoD 5200.08-R, Physical Security Program; AR 25-2, Information Assurance; AR 190-8, Enemy Prisoners of War, Retained Personnel, Civilian Internees and Other Detainees; and AR 525-13, Antiterrorism.

Purpose(s):
To facilitate biometric identification (i.e., automated identity verification of individuals by reference to their measurable physiological and/or behavioral characteristics) of U.S. Persons who seek access to DoD property, installations, or information; U.S. Persons who pose a threat to DoD personnel, assets or missions, or to national security; U.S. Persons who are captured, detained, or otherwise encountered by DoD forces during military operations; and U.S. Persons for whom DoD has the responsibility to recover or account during or as a result of DoD operations. Information is collected to support DoD military missions, detainee affairs, personnel recovery, force protection,

antiterrorism, special operations, stability operations, homeland defense, counterintelligence, and intelligence efforts around the world.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To Federal, State, tribal, local, foreign or international agencies, task forces or organizations, for the purposes of law enforcement, counterterrorism, immigration management and control, force protection, personnel recovery and homeland security as authorized by U.S. Law or Executive Order; or for the purpose of protecting the territory, people, and interests of the United States of America against breaches of security related to DoD controlled information or facilities.

To those federal agencies that have agreed to provide support to DFBA for purposes of ensuring the continuity of DFBA operations.

To any Federal, State, tribal, local, territorial, foreign, or multinational agency, entity or organization that is engaged in, or is planning to engage in, terrorism screening, or national security threat screening, authorized by the U.S. Government, for the purpose of development, testing, or modification of information technology systems used or intended to be used during or in support of the screening process; whenever practicable, however, DFBA, to the extent possible, will substitute anonymized or de-identified data, such that the identity of the individual cannot be derived from the data.

To any person or entity in either the public or private sector, domestic or foreign, when reasonably necessary to elicit information or cooperation from the recipient for use by DFBA in the performance of an authorized function, such as obtaining information from data sources as to the thoroughness, accuracy, currency, or reliability of the data provided so that DFBA may review the quality and integrity of its records for quality assurance or redress purposes, and may also assist persons misidentified during a screening process.

To any Federal, State, tribal, local, territorial, foreign,

multinational agency or task force, or any other entity or person that receives information from the U.S. Government for terrorism screening purposes, or national security threat screening purposes, in order to facilitate DFBA's or the recipient's review, maintenance, and correction of DFBA data for quality assurance or redress purposes, and to assist persons misidentified during a screening process.

To any agency, organization or person for the purposes of (1) performing authorized security, audit, or oversight operations of the DoD, OPMG, DFBA, or any agency, organization, or person engaged in or providing information used for terrorism screening, or possible national security threat screening, that is supported by DFBA, and (2) meeting related reporting requirements.

The Blanket Routine Uses set forth at the beginning of the Army's compilation of systems of records notices may apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:
Paper records in file folders and electronic storage media.

Retrievability:
Name, DNA, biometric template, fingerprints, facial image, iris image.

Safeguards:
Computerized records are maintained in a controlled area accessible only to authorized personnel. Physical entry is restricted by the use of locks and guards, and is permitted only to authorized personnel. Physical and electronic access is restricted to designated individuals requiring such access in the performance of official duties. Access to computerized data is restricted by use of common access cards (CACs), and is permitted only to users with authorized accounts. The system and electronic backups are maintained within controlled facilities that employ physical restrictions and safeguards such as security guards, identification badges, key cards and locks.

Retention and disposal:
Records in this system will be retained and disposed of in accordance with the records schedule approved by the National Archives and Records Administration. In general, records in the Automated Biometric Identification System are destroyed

seventy-five years after the end of the calendar year in which the record was submitted or last updated, or when they are no longer needed for military operations or DoD business functions, whichever is later.

System manager(s) and address:
Director, Defense Forensics and Biometrics Agency, 251 18th Street South, Suite 244, Arlington, VA 22202-3532.

Notification procedure:
Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to Director, Defense Forensics and Biometrics Agency, 251 18th Street South, Suite 244, Arlington, VA 22202-3532.

The requester should provide full name, current address and telephone number, and signature.

In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: 'I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).'

If executed within the United States, its territories, possessions, or commonwealths: 'I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).'

Record access procedures:
Individuals seeking access to information about themselves contained in this system should address written inquiries to Director, Defense Forensics and Biometrics Agency, 251 18th Street South, Suite 244, Arlington, VA 22202-3532.

The requester should provide full name, current address and telephone number, and signature.

In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: 'I declare (or certify, verify, or state) under penalty of perjury under the laws of

the United States of America that the foregoing is true and correct. Executed on (date). (Signature).'

If executed within the United States, its territories, possessions, or commonwealths: 'I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).'

As a matter of policy, the Department of Homeland Security extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals seeking notification of, access to, or seeking to contest the content of Department of Homeland Security information may submit a request using the procedure outlined in Department of Homeland Security/NPPD-004 DHS Automated Biometric Identification System, System of Records, available at www.dhs.gov/privacy.

Contesting record procedures:
The Army's rule for accessing records, contesting contents, and appealing initial agency determinations are contained in Army Regulation 340–21; 32 CFR part 505; or may be obtained from the system manager.

Record source categories:
Data is collected from existing DoD databases, the Military Services, DoD Components, the individual; from other federal, state, and local government agencies such as the Federal Bureau of Investigation (FBI) (to include the FBI Terrorist Screening Center (TSC)), the Department of State and Department of Homeland Security in accordance with applicable law, policy, agreements, and published routine uses; and from foreign government agencies and international organizations in accordance with applicable law, policy, and agreements.

Exemptions claimed for the system:
Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws.

Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for

which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

Exempt materials from JUSTICE/FBI-019 Terrorist Screening Records System and/or other sources listed above may become part of the case records in this system of records. To the extent that copies of exempt records from JUSTICE/FBI-019, Terrorist Screening Records System, and/or other sources listed above are entered into these case records, the Department of the Army hereby claims the same exemptions, (j)(2) and (k)(2) for the records as claimed in JUSTICE/FBI-019, Terrorist Screening Records system of records of which they are a part as reflected in the final rule published on June X, 2014, XX FR XXXXX.

To the extent that copies of exempt records from other sources may become part of these records, the Department of the Army hereby claims the same exemptions for such records as claimed at their source.

An exemption rule for this exemption has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 505. For additional information contact the system manager.