PRIVACY IMPACT ASSESSMENT (PIA)

For the

Department of Defense Automated Biometrics Identification System (DoD ABIS)
United States Army

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 15478/DA207770
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier A0025-2 DoD PMG

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office 1 DEC 14
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ **Yes**

Enter OMB Control Number 0702-0127

Enter Expiration Date

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; National Defense Authorization Act of 2008, Section 1069; Public Law 106-246, Section 112, Emergency Supplemental Act; 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; DoD Directive 8521.01E, Department of Defense Biometrics; DoD Directive 8500.1, Information Assurance (IA); DoD Instruction 8500.2, Information Assurance Implementation; Army Regulation 25-2, Information Assurance; DoD Directive 2310.7, Personnel Accounting-Loses Due to Hostile Acts; Army Regulation 190-8, Enemy Prisoners of War, Retained Personnel, Civilian Internees and Other Detainees; DoD Directive 5110.10, Defense Prisoner of War/Missing in Action Office; DoD Instruction 2310.5, Accounting for Missing Persons; and E.O.9397 (SSN); DoDI 2000.12, DoD Antiterrorism (AT) Program; DoDI 5200.08, Security of DoD Installations and Resources; DoD 5200.08-R, Physical Security Program; and Army Regulation 525-13, Antiterrorism; Deputy Secretary of Defense Memorandum, "Executive Agent for the Department of Defense (DoD) Biometrics Project"; Deputy Secretary of Defense Memorandum, "Authority to Collect, Store, and Share Biometric Information of Non-U.S. Person with U.S. Government Entities and Partner Nations" (13 JAN 2012).

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The Department of Defense Automated Biometric Identification System (DoD ABIS) supports Identity Superiority, which is defined as the management, protection, and dominance of identity information associated with friendly, neutral/unknown, and adversary individuals across military operations and business functions under three types of identity missions, defined below:

(1) Identity Dominance – is the operational capability to achieve an advantage over an adversary by denying him the ability to mask his identity or counter our biometric technologies and processes. Enabling technologies and processes establish the true identity of an individual and a knowledge base for that identity.
(2) Identity Management – is a business function that securely authenticates an individual to validate identity, DoD affiliation, and validity of the credential holder. The centralized repository delivers credentialing information and status for business functions within DoD for use as proof of identity and DoD affiliation.
(3) Identity Protection – is the process of safeguarding identities and ensuring that the identities of individuals, devices, applications, and services are not compromised.

In order to support the missions mentioned above, DoD ABIS has five subprocesses:
• Receive/Process – Receive biometric data collected from collection assets by various government programs and systems and process data based on Electronic Biometric Transmission Specification/ Electronic Fingerprint Transmission Specifications (DoD EBTS/EFTS) standards as a central repository.
• Store - Update, and maintain biometric files to make standardized, current biometric information of individuals available when and where required.
• Match - Accurately identify or verify the identity of an individual by comparing a standardized biometric file to an existing source of standardized biometrics data and scoring the level of confidence of the match. Matches can be conducted 1:1 or 1:Many.
• Share - Exchange standardized biometric files and match results among approved DoD, Interagency and Multinational partners, in accordance with applicable law and policy.
• Decide/Act – Allows users to take action based on the match results of a biometric file and in connection with references and analysis from repositories of non-biometric information on individuals.

DoD ABIS also enables DoD to provide associated testing, system development, and performance and administrative analysis to improve the identification of individuals based on biographic and biometric information.

Within this release, DoD ABIS focuses on achieving Identity Dominance and Identity Management over neutral/unknown and adversary population groups. Future releases will enhance existing capabilities and support Identity Protection.

DoD ABIS stores biometric data, such as fingerprint, latent palm print, iris, and facial photograph; biographic information such as name, national origin, address, identification numbers, family relationships, religion; and contextual information such as location of data collection.

The type of PII collected is personal, medical, military, employment, and law enforcement.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks associated with DoD ABIS include the inappropriate denial of freedom of movement, or access to logical and physical assets. These risks may result from unauthorized collection, use, disclosure and retention of personal information, and insufficient data quality.

Unauthorized collection and use can occur when systems that provide information to DoD ABIS exceed their authority for collection. Once information is submitted, 1) errors or omissions in the data regarding an

individual's citizenship may result in some US Persons records not being identified and handled appropriately, 2) contextual data may be inappropriately interpreted as derogatory, and 3) inaccurate biometric matching may result in false acceptance and false rejection. False acceptance occurs when a biometric system incorrectly identifies a biometric subject or incorrectly authenticates an imposter against a claimed identity, such as allowing an individual who shouldn't have access to a military base onto a military base. False rejection occurs when the failure of a biometric system to identify a biometric subject or to verify the legitimate claimed identity of a biometric subject, such as denying an individual who should have access to a military base from a military base.

Established policies and procedures minimize these privacy risks. DoD ABIS promotes the authorized use of personal information by only accepting data and search requests from authorized agencies and limiting search responses to match/no match with associated, unverified biographical information. DoD subject matter experts are available to determine whether contextual data associated with a match is derogatory. DoD ABIS promotes data quality by comparing data types from more than one source when updating the data, using the highest quality biometrics for matching, and continually testing algorithms to improve the system's biometric matching capabilities. DoD ABIS secures the personal information with multiple layers of logical access controls. The storage systems are physically isolated from external access and are logically located behind three firewalls. A Network-based Intrusion Detection System and a Host-based intrusion detection system have been implemented. In addition, rigorous physical access controls have been implemented, including security personnel and biometric identification systems.

Records ingested into ABIS from authorized agencies are sometimes categorized as Search and No Retain (SANR), to indicate that after the data is searched for a match, it shall be deleted from the database. As ABIS does not have the automated capability or the manpower hours necessary to regularly expunge the SANR records, the information is retained within the transaction manager. In certain instances, data sources can be altered to indicate that files should thereafter be ingested as SANR, where previously they were not. If this is the case, data ingested prior to the change is not able to be handled as SANR in ABIS.

Though SANR records are not fully expunged, the data exists solely within the transaction manager, not the biometric database. Furthermore, the data in the transaction manager is not the match/identity or biometric data, but instead the candidate and/or score data documenting the transaction. No match/identity/biometric data is stored in the database. The transaction manager does not allow for automated searching of data, thus, this candidate and/or score information about the transaction is only discoverable by manual methods. In the case that a data source is later flagged as SANR, ABIS operators notify DFBA Policy Branch, who coordinate with the agency or organization directly to make an official determination to delete, retain, or re-categorize the older submissions.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. Appropriate safeguards are in place for the collection, use and safeguarding of information.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Defense Forensics and Biometrics Agency (DFBA) Biometrics Identity Management Activity (BIMA); National Ground Intelligence Center(NGIC)

☒ **Other DoD Components.**

Specify. All Combatant Commands (CCMDs); Navy; Marine Corps; Air Force; Defense Intelligence Agency (DIA)

☒ **Other Federal Agencies.**

Specify. Federal Bureau of Investigation, Department of State, Department of

Homeland Security, Terrorist Screening Center, National Defense Research Committee (NDRC)

☒ **State and Local Agencies.**

Specify. Texas Department of Public Safety

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. "15.9 Privacy Act
Work on this project requires that personnel have access to Privacy Information. All Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations (http://www.justice.gov/opcl/privstat.htm)."

☒ **Other** (e.g., commercial providers, colleges).

Specify. United Kingdom Ministry of Defence; Canada Department of National Defence; Islamic Republic of Afghanistan Ministry of the Interior; Republic of Kosovo Ministry of Internal Affairs; Republic of Kenya Ministry of Defence; Cape Verde Judicial Police; Germany Ministry of Defense

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

Data in DoD ABIS is collected by various government programs and systems, and then transmitted to DoD ABIS. DoD ABIS relies on the initial collector to provide an opportunity to object to collection, as appropriate, based on the purpose for which the information is collected. An opportunity to object is generally provided when personal information is used for administrative purposes such as granting access to logical or physical assets. However, for certain military and intelligence operations, an opportunity to object to collection may undermine the DoD mission, and therefore it is not provided.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.