PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Department of Defense Automated Biometrics Identification System (DoD ABIS)

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

Project Manager DoD Biometrics

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

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

The Department of Defense Automated Biometrics Identification System (DoD ABIS) is the DoD's only authoritative biometric repository established to support DoD's Identity Superiority mission. Identity Superiority is defined as identity information dominance, management, and protection collected from potential threat actors across full range of military operations under the three types of identity missions, defined below:

(1) Identity Dominance – 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/repository for identities.
(2) Identity Management – 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 within DoD for use as proof of identity, DoD affiliation and in support of DoD force protection mission, and intelligence.
(3) Identity Protection – The process of safeguarding identity data and ensuring that information regarding individuals, devices, applications, methods and services are not compromised.

In order to support the missions mentioned above, DoD ABIS has four major functions:
(1) Receive/Process – Receive biometric data collected from collection assets by various government programs and systems to process data in the central repository based on Electronic Biometric Transmission Specification (EBTS) as well as other standards.
(2) Match - Accurately identify or verify the identity of an individual by comparing a standardized biometric file to the repository of standardized biometrics data and scoring the level of confidence of each match as either 1:1 or 1:Many.
(3) Store - Process current biometric information of individuals available when and where required.
(4) Share - Exchange standardized biometric files and match results among approved DoD, Interagency and Multinational partners, in accordance with applicable law, policy and data sharing agreements.

DoD ABIS stores biometric data, such as fingerprint, latent palm print, iris, and facial photographs; 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 military, employment, and law enforcement. DoD ABIS is intended to search, match and store data for potential threat actors, typically Non-U.S. Persons, for which the U.S. Privacy Act law does not apply. However, there can be rare situations where a U.S. Person is submitted to DoD ABIS for search, match, and store. The DoD ABIS accepts submissions from collectors who have made the decision whether or not to send a U.S. Person to DoD ABIS.

DoD ABIS consists of two environments: the primary location, named the Operational Environment (OE) and a backup location, named the Disaster Recovery System (DRS). Identical data is housed at both locations as the OE replicates data to the DRS continually.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

DoD ABIS uses submitted Biometrics (Fingerprints, Iris, Face and Palm) to identify and verify known or suspected threat actors worldwide in support of DoD's force protection, law enforcement and military Operations.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

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

(2) If "No," state the reason why individuals cannot object to the collection of PII.

DoD ABIS repository does not collect PII from individuals, however, various Government programs and systems collect Biometric data, including PII, and directly transmits to DoD ABIS. The initial collector provides 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 force protection 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.

f. 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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Individual rights are afforded in accordance with applicable law. Whether an individual has the opportunity to consent to specific uses of their PII will vary based on the particular purpose associated with the initial collection of the information and in accordance with statutory requirements for the various Government programs and biometric collection system.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

The initial collectors from the various Government programs and biometric collection systems are responsible for providing a Privacy Act Statement or Privacy Advisory when appropriate. The extent of the notice provided will vary based on the purpose for which the information was collected.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	Defense Forensics and Biometrics Agency Biometrics Operations Division (DFBA BOD); 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 *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	"15.9 Privacy Act Work on this project requires contractor personnel to 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. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☐ Individuals ☒ Databases

☒ Existing DoD Information Systems ☐ Commercial Systems

☒ Other Federal Information Systems

DoD ABIS is able to ingest data through the use of computer attached storage (disks, tapes, other computer accessible media) that may originate in other information systems and/or databases from DoD and other Federal agencies and coalition partners.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [x] E-mail
- [ ] Face-to-Face Contact
- [ ] Fax
- [x] Information Sharing - System to System
- [x] Other *(If Other, enter the information in the box below)*
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [x] Paper
- [ ] Telephone Interview
- [ ] Website/E-Form

DoD ABIS is able to ingest data through the use of computer attached storage (disks, tapes, other computer accessible media) that may originate in other information systems and/or databases from DoD and other Federal agencies and coalition partners.

k. 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 must be consistent.

- [x] Yes
- [ ] No

If "Yes," enter SORN System Identifier TBD

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

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; 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).

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☐ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0702-0127

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

[X] Biometrics	[X] Birth Date	[ ] Child Information
[X] Citizenship	[X] Disability Information	[X] DoD ID Number
[ ] Driver's License	[ ] Education Information	[ ] Emergency Contact
[X] Employment Information	[ ] Financial Information	[X] Gender/Gender Identification
[X] Home/Cell Phone	[X] Law Enforcement Information	[ ] Legal Status
[X] Mailing/Home Address	[X] Marital Status	[ ] Medical Information
[X] Military Records	[X] Mother's Middle/Maiden Name	[X] Name(s)
[X] Official Duty Address	[X] Official Duty Telephone Phone	[X] Other ID Number
[X] Passport Information	[X] Personal E-mail Address	[X] Photo
[X] Place of Birth	[ ] Position/Title	[ ] Protected Health Information (PHI)[1]
[X] Race/Ethnicity	[ ] Rank/Grade	[X] Religious Preference
[ ] Records	[X] Security Information	[ ] Social Security Number (SSN) *(Full or in any form)*
[ ] Work E-mail Address	[X] If Other, enter the information in the box below	

The information can contain scars, marks and tattoos; Personal Identification Number, Government ID, DoD Defense Biometrics Identification System ID, Dossier Number, Federal Bureau of Investigation Number, Biometric Automated Toolset Globally Unique Identifier, and Internment Serial Number

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

[ ] Yes [X] No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

There is no SSN Justification Memo. DoD ABIS is not required to collect, maintain, use nor disseminate SSNs.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

N/A

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

N/A

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

[ ] Yes [X] No

N/A as DoD ABIS does not collection, maintain, use and /or disseminate SSNs, therefore a plan to eliminate their usage is not applicable.

b. What is the PII confidentiality impact level[2]? [ ] Low [X] Moderate [ ] High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [x] Cipher Locks
- [ ] Combination Locks
- [x] Key Cards
- [x] Security Guards
- [x] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [x] If Other, enter the information in the box below

DoD ABIS is housed in the Biometric Technology Center (BTC) located within the FBI CJIS Campus in West Virginia. There are multiple levels of physical security: 1) CJIS Campus security check point, 2) Building security check point for access to the BTC Building, and 3) DFBA BOD Facility security check point for access to the DFBA BOD and DoD ABIS assets located in the BTC. The Cloud-deployed portion of DoD ABIS resides in the Amazon Web Services cloud. Amazon is responsible for the physical security of their facilities.

(2) Administrative Controls. *(Check all that apply)*

- [ ] Backups Secured Off-site
- [x] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [ ] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

The System Owner, Product Manager Biometrics Enabling Capability (PdM BEC), is responsible for the implementation, fielding, and maintenance of technical solutions that meet Warfighter and DoD requirements, including the ability to encrypt backups made by the system, and periodic security audits in support of the Authority to Operate. The System Operator, Defense Forensics Biometrics Agency (DFBA), is responsible for the physical security and facilities for the system, as well as personnel access to the system, security of backups removed from the system, and training of personnel.

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [x] Encryption of Data at Rest
- [x] Firewall
- [x] Role-Based Access Controls
- [x] Virtual Private Network (VPN)
- [x] Command Access Card (CAC)
- [x] Encryption of Data in Transit
- [x] Intrusion Detection System (IDS)
- [ ] Used Only for Privileged (Elevated Roles)
- [x] If Other, enter the information in the box below
- [x] DoD Public Key Infrastructure Certificates
- [x] External Certificate Authority Certificates
- [x] Least Privilege Access
- [x] User Identification and Password

DoD ABIS employs numerous cybersecurity technical controls based on the Risk Management Framework process governed by NIST 800-53 and DOD 8510.01 to ensure the technical security of the system. Additional measures include use of HBSS and ACAS to continuously monitor and manage the security posture of the system. DoD ABIS also measures software code vulnerability through the use of HP Fortify and Steel Cloud software assurance tools and conducts independent Software Assurance Assessments.

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

DoD ABIS also monitors incoming submissions from external partners, analyzes the messages for any SSNs that may be erroneously present, and removes them from the data prior to the data being ingested, processed, or stored by the DoD ABIS system.