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:

Identity Authentication Services (iAS)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

04/23/2026

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

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

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☒ 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.

Identity Authentication Services (iAS) provides an array of standardized Identity Governance and Administration (IGA) services for authentication and authorization of Uniformed Services personnel, Retirees and their beneficiaries to determine their level of access to Military Health System (MHS) applications. iAS services include account provisioning, federated identity service, Public Key Infrastructure (PKI) enablement, Certificate Authority (CA) validation, Single Sign On (SSO), user registration and account management.

Personally Identifiable Information (PII) may include numerous types of PII including employee and beneficiary contact information, military information, demographic information, Social Security Number (SSN), and Protected Health Information (PHI).

iAS is owned and maintained by the DHA's Solution Delivery Division (SDD).

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)*

The collected PII is used by iAS to authenticate and authorize users into MHS applications to support resource/benefit management, and critical defense missions.

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.

When using iAS to authenticate into a system, iAS is not the initial point of collection, individuals do not have the opportunity to object to the collection of their PII. When using iAS to enter an online 2875 access request, depending on the method of authentication into iAS IdentityIQ, additional profile information may need to be collected. They cannot proceed with requesting access to a system without providing their Rolodex PII (Name, Work address, Work phone number, Job Title, and Email) which is a requirement for any 2875 access request. Not providing this data or entering "N/A" may delay or prevent the processing of their access request.

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.

When using iAS to authenticate into a system, iAS is not the initial point of collection, individuals do not have the opportunity to object to the collection of their PII. When the users authenticate into iAS IdentityIQ to enter an online 2875 access request, depending on the method

of authentication, additional profile information may need to be collected. They cannot proceed with requesting access to a system without consenting to providing their Rolodex PII (Name, Work address, Work phone number, Job Title, and Email) which is a requirement for any 2875 access request. Not providing this data or entering "N/A" may delay or prevent the processing of their access request.

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

PRIVACY ADVISORY:
You are accessing a U.S. Government information system (IS) which may contain information subject to the Privacy Act of 1974, as amended, 5 U.S.C. § 552(a). By accessing this system, you: (1) acknowledge that you possess a valid need-to-know; (2) agree to adhere to all applicable DoD & DHA requirements concerning access to information subject to the Privacy Act of 1974; and (3) acknowledge that disclosure of protected Privacy Act information in this IS, in any manner, to person(s) or entity(ies) not entitled to receive it, may subject you to administrative, civil, and/or criminal penalties.

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

☒ Within the DoD Component	Specify.	DHA Military Treatment Facilities (MTF's), DMACS 2.0, JLVWEB, ESSENCE, BCS, PHIMT, PEPR
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Defense Manpower Data Center (DMDC)
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Veterans Affairs (VA)
☐ State and Local Agencies	Specify.	
☐ 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.	
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

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

Defense Enrollment Eligibility Reporting System (DEERS)
iAS Enterprise Common Access Card (CAC) Registration System (ECRS), iAS IdentityIQ

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

☐ E-mail ☐ Official Form (*Enter Form Number(s) in the box below)*
☐ In-Person Contact ☐ Paper
☐ Fax ☐ Telephone Interview
☒ Information Sharing - System to System ☒ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier DoD 0015

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.

Mission Schedules:
- 1601-02: GRS 3.2, item 030 (DAA-GRS-2013-0006-0003)
- 1606-12: GRS 3.2, item 060 (N1-GRS-07-3, item 13a (1))
- 1606-13: GRS 3.2, item 061 (N1-GRS-07-3, item 13a (2))
- 1606-14: GRS 3.2, item 062 (N1-GRS-07-3, item 13b)

Other Schedules:
- Data Administration and Documentation: GRS 3.1, item 051 (DAA-GRS-2013-0005-0003)

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

(3) Retention Instructions.

Mission Schedules:
FILE NUMBER: 1601-02
FILE TITLE: System Access Records - Systems not requiring Special Accountability for Access
DISPOSITION: Temporary. Cut off and destroy when business use ceases. NOTE: See 1601-18 for System Access Records Requiring Special Accountability

FILE NUMBER: 1606-12
FILE TITLE: Public Key Infrastructure (PKI) Administrative Records – Federal Bridge Certification Authority (FBCA) Certification Authority
DISPOSITION: Temporary. Cutoff annually. Destroy 7 years and 6 months, 10 years and 6 months, or 20 years and 6 months after cutoff, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.

FILE NUMBER: 1606-13
FILE TITLE: Public Key Infrastructure (PKI) Administrative Records – Non-Federal Bridge Certification Authority (Non-FBCA) Certification Authority
DISPOSITION: Temporary. Cut off annually. Destroy 7 years 6 months to 20 years 6 months after cutoff, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.

FILE NUMBER: 1606-14
FILE TITLE: Public Key Infrastructure (PKI) Transaction-Specific Records
DISPOSITION: Temporary. Cut off annually. Destroy 7 years 6 months to 20 years 6 months after cutoff, based on the maximum level of operation of the appropriate CA and after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule, or in the case of permanent records, when the record is transferred to NARA legal custody.

Other Schedules:

FILE NUMBER: 1601-12
FILE TITLE: Data Administration and Documentation - Temporary Systems
DISPOSITION: Temporary. Cut off after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system. Destroy 5 years after cutoff.

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.

10 U.S.C. 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; 10 U.S.C. 2224, Defense Information Assurance Program; 10 U.S.C. Chapter 8-Defense Agencies and Department of Defense Field Activities; 31 U.S.C. 902, Authority and functions of agency Chief Financial Officers; Homeland Security Presidential Directive (HSPD) 12, Policies for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management; National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors; DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense; DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense; and DoD Instruction 8520.03, Identity Authentication for Information Systems

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.

iAS does not require OMB approval per DoD Manual 8910.01, volume 2, "DoD information collections manual", as it is not the initial point of PII collection.