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:

DoD Mobility Unclassified Capability (DMUC)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

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

☐ 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

☒ 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.

In an effort to evolve the DoD IT enterprise, DISA is pursuing the development of two Assured Identity Pilots, Qualcomm and TWOSENSE, to provide a more robust identification and authentication scheme while enhancing user-friendliness with respect to user access to work environments on production networks. This effort has two specific goals: prototype the means for device and key attestation and Continuous Multifactor Authentication (CMFA) implemented on a prototype device that will be used in a limited pilot across the DoD.

Qualcomm Information collected will include:
1. Facial recognition
2. Finger-print
3. Gait
4. Voice
5. GPS
6. Bluetooth
7. Trusted network

TWOSENSE behavioral biometric information collected, encrypted, and stored in an AWS cloud will include:
1. Motion Sensor Data
2. Ambient Environment Sensor Data
3. Geo-location and Radios Data
4. Device Information Settings
5. User Interaction Data
6. Authentication Events Data
7. Debugging & Troubleshooting Data

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)*

Behavioral biometrics will be collected to continuously identify and authenticate users.

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.

All users will be from the testing group and opt into the program. Once users consent to enrolling credentials on the device inherently behavior biometrics will be collected and stored on the device (Qualcomm) and in the cloud (TWOSENSE).

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.

Users in the Assured Identity program will have their biometric data used for identification and authentication. They will not be able to consent to specific types of PII.

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

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.	
□ Other DoD Components	Specify.	
□ Other Federal Agencies	Specify.	
□ 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.	TWOSENSE: Contract personnel shall be capable of accessing, handling, receiving, and storing UNCLASSIFIED documents, equipment, hardware, and test items, using the applicable standards of FOUO and CUI. DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting applies to this effort.
☒ Other *(e.g., commercial providers, colleges).*	Specify.	Qualcomm: The information will not leave the device and cannot be seen by administrators

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals

□ Existing DoD Information Systems

□ Other Federal Information Systems

□ Databases

□ Commercial Systems

Collecting personal biometric data

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

□ E-mail

□ Face-to-Face Contact

□ Fax

□ Information Sharing - System to System

☒ Other *(If Other, enter the information in the box below)*

□ Official Form (*Enter Form Number(s) in the box below)*

□ Paper

□ Telephone Interview

□ Website/E-Form

(Qualcomm) - Information is obtained and maintained on the Mobile device only
(TWOSENSE) - Behavior biometric information is securely transported to the cloud and encrypted in the cloud.

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 K890.31

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.

SORN is required to be completed and Published in the Federal Register for 30 days before a system can begin to collect PII.
SORN brief: https://disa.deps.mil/disa/cop/Privacy_Act/PLASORN%2020Brief/Forms/AllItems.aspx
SOR Template: https"//disa.deps.mil/disa/cop/Privacy_Act/PLASORN%20Brief/Forms/AllItems.aspx

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.

An SF115 will be submitted to NARA upon completion of the Information Systems Description form, the Program Manager must complete and send back to ARO.

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.

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.

30 Jan 2019