

## 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 NIPR LAB

**2. DOD COMPONENT NAME:**

Defense Information Systems Agency

**3. PIA APPROVAL DATE:**

5/3/2022

### 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.**

The NIPR Lab is a Zone A, preproduction environment. The purpose of the NIPR Lab is to evaluate Mobile solutions in a preproduction environment. NIPR Lab can only be accessed inside the lab.

Commercial Lab is a Zone D, preproduction environment. The purpose of the Commercial Lab is to evaluate Mobile solutions in a preproduction environment. Only certain services in the Commercial lab are exposed to the Internet, such as the MobileIron Core's Admin Console. The majority of commercial systems can only be accessed via the commercial lab's VPN or in the lab. The Core's Admin console requires certificate based authentication, utilizing certs issued off of the JITC OM CAs.

NGD Lab is a Zone D, preproduction environment. The purpose of the NGD Lab is to evaluate Mobile solutions in a preproduction environment. Remote access is only available through an Out-of-Band network, protected by a VPN. This VPN access is further restricted through the use of Multifactor Authentication; username/password and a one-time password (time based) OTP.

Only names are collected within the system labs.

**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)

Names are collected to identify the users accessing the system labs.

**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.

Names are collected to identify the users accessing the system labs. Users must sign a DOD 2875 before access is granted.

**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.

Names are collected to identify the users accessing the system labs. Users must sign a DOD 2875 before access is granted.

**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

Authority - Executive Order 10450, and Public Law 99-474, the Computer Fraud and Abuse Act.

Principal Purpose - To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

Routine Uses - None

Disclosures - Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

**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.    DISA
- Other DoD Components (i.e. Army, Navy, Air Force)      Specify.
- Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)      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.
- 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

**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)

DoD 2875

**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    K890.15

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.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.

**I. 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. GRS 3.2 #62 (N1-GRS-07-3, item 13b)

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

(3) Retention Instructions.

Temporary. Destroy/delete when 7 years 6 months to 20 years 6 months old, 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. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period.

**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 statute 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.

The following authority allows Mobility NIPR Lab collect the data:

10 U.S.C. Chapter 8, Defense Agencies and Department of Defense Field Activities

DoD Directive 5105.19, Defense Information Systems Agency (DISA)

DoD Instruction (DoDI) 1000.25, DoD Personnel Identity Protection (PIP) Program

DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)

DoDI 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.

OMB Control Number: 0704-0415; Expiration Date: None