

## 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:**

Maintenance, Repair and Overhaul Initiative (MROi)

**2. DOD COMPONENT NAME:**

United States Air Force

**3. PIA APPROVAL DATE:**

05/26/20

### SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- |   |   |
|---|---|
| <input type="checkbox"/> From members of the general public   | <input checked="" type="checkbox"/> From Federal employees and/or Federal contractors |
| <input type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4)              |

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

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> New DoD Information System         | <input type="checkbox"/> New Electronic Collection      |
| <input type="checkbox"/> Existing DoD Information System               | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.**

MROi is a new tool for managing Depot Maintenance. Information is gathered for maintainers who perform the work and is used to verify certification for work performed and tracking hours worked on items undergoing depot-level maintenance repair and/or overhaul. Each record will contain the following PII data elements Full Name, DoD ID Number, Position/Title, Work E-mail address, and maintenance certification status information on individuals.

**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)

Verification of certifications for work to be performed, reporting maintenance on-work time

**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.

Individuals can voluntarily choose not to disclose information on the MROi System Authorization Access Request (SAAR) DD Form 2875. However, if they do choose not to disclose the required information, the individual is denied access to MROi.

**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.

Routine uses of the information provided are stated on the MROi System Authorization Access Request (SAAR) DD Form 2875. Individuals can voluntarily choose not to disclose information on the MROi System Authorization Access Request (SAAR) DD Form 2875. However, if they do choose not to disclose the required information, the individual is denied access to MROi.

**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.)

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory | <input checked="" type="checkbox"/> 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.
- 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

Individuals - System Authorization Access Request (SAAR) DD Form 2875  
Existing DoD Information Systems - Training Scheduling System (TSS) for Maintainer Certifications

**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)
- Face-to-Face Contact       Paper
- Fax       Telephone Interview
- Information Sharing - System to System       Website/E-Form
- Other (If Other, enter the information in the box below)

Official Form - System Authorization Access Request (SAAR) DD Form 2875  
Information Sharing - Training Scheduling System (TSS) for Maintainer Certifications

**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

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.

MROi receives maintenance certification status information via an approved automated system interface with the authoritative data source (ADS), Training Scheduling System (TSS). Maintenance certification status of individuals is considered PII, but is not subject to the provisions of the Privacy Act. The requirements of the Privacy Act are triggered by the retrieval of information by use of a name or other identifier assigned to an individual. The collected maintenance certification status information is retrieved from the ADS and associated with existing MROi user records in the system by a back-end database process. Maintenance certification status information is not retrieved in the MROi application by use of a name or other identifier assigned to an individual.

**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.

Table & Rule 21-05 R 02.00: Depot Maintenance and Inspection Records--Destroy 6 months after receipt of notification of acceptance or 6 months after turn in of equipment to supply (N.B. Records under this disposition are \*frozen\* and must \*not\* be destroyed due to the functional proposal to extend the retention time and gain the approval of the National Archives and Records Administration for the change.)

**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.

AFI 36-2650, Maintenance Training; AFMCI 21-100, Depot Maintenance Management; and AFSCMAN 21-102, ENGINEERING DATA STORAGE, DISTRIBUTION, CONTROL, AND CONFIGURATION CONTROL

**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.

MROI is not collecting data from the public

**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)

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

(Other) Maintenance certification status information required for the work being performed.

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     No

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

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

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

(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     No

**b. What is the PII confidentiality impact level<sup>2</sup>?**     Low     Moderate     High

<sup>1</sup>The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.  
<sup>2</sup>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.

NOTE: Sections 1 above is to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy. A Component may restrict the publication of Sections 1 if they contain information that would reveal sensitive information or raise security concerns.