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:

Training Scheduling System (TSS)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

08/24/20

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
- [x] 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
- [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.

Used to track and schedule maintenance training and Personnel Accreditation Certification (PAC). The personal information collected is: first name.last, rank/grade, series type, org id, pay plan, location, title, managerID, empTypid, work email, DSN, and EDIPIs. This information is used to setup training plans for individuals based on their series (skill), grade and organization.

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 type of individual information collected is used to track the training and certification of USAF/DOD personnel.

e. Do individuals have the opportunity to object to the collection of their PII? [x] 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.

The user can object, but will not be allowed access to the TSS application.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

This information is required to authenticate the individual user into the TSS application.

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
- [x] Privacy Advisory
- [ ] Not Applicable

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
• The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
• At any time, the USG may inspect and seize data stored on this IS.
• This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
• Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.
Additionally, TSS displays Privacy Advisory and Accessibility/Section 8 Compliance language accessible on the TSS home page.

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

[X] Within the DoD Component	Specify.	Education and Training Management Systems (ETMS), Maintenance Repair and Overhaul initiative (MROi), & Maintenance Business System Modernization (MABSM).
[ ] 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)*

- [X] 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)*

- [X] E-mail
- [X] Official Form (*Enter Form Number(s) in the box below)*
- [X] 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)*

All TSS user's complete a DD FM 2875 for system access. All relevant information for system access to TSS is taken from this form.

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 [X] No

If "Yes," enter SORN System Identifier n/a

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.

Social Security Numbers (SSNs), were removed from the system on 8 Mar 2019. TSS will no longer collect or house individuals SSNs.

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. N1-AFU-96-12, N1-AFU

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

(3) Retention Instructions.

Retained IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule:
T32 - 35 R01.00 - Fire Department Training; Destroy when individual is certified at next higher level.
T36 - 28 R04.00 - Training Through Installation Facilities Individ. Course Folders, Training Through Other Than Installation Facilities; Destroy 2 years after course is completed.
T36 - 28 R07.00 - Annual Report of Civilian Training & Supplemental Records Relating to Expenses, Apprentice Action @ Other Than HQ USAF; Destroy when 3 years old.
T36 - 28 R08.02 - Career Enhancement Plan (CEP); When used as a training survey document in lieu of the annual training, development or financial plans, destroy after 5 years, otherwise destroy when updated.
T36 - 37 R09.00 - Training Instructions; Destroy immediately after reassignment or separation.
T36 - 38 R10.00 - Explosive ordnance disposal (EOD) Proficiency Training Records; Destroy 24 months after training completion, when superseded by additional training, or when the training requirement is eliminated.
T36 - 38 R14.00 - Maintenance Training Worksheets at management or training control; Destroy upon completion of training and when files are no longer needed.
T36 - 36 R15.00 - Survivor Benefit Plan (SBP); Documents are retained in the UPRG and should be disposed IAW AFI 36-2608.
T36 - 38 R16.00 - Maintenance Proficiency Tests, ICBM Production Inspector Records; Destroy when superseded, obsolete, no longer needed, or when individual is reassigned
T36 - 38 R19.00 - Individual Proficiency Evaluation Filed in Training Record, Maintenance Standardization & Evaluation in Training Record; Destroy when replaced by next equivalent evaluation.
T36 - 38 R20.00 - Training Request/Completion Notification; Destroy after training is completed and posted to applicable record.
T36 - 38 R23.01 - Maintenance and Standardization and Evaluation Training Visibility, Other Maintenance Records; Destroy after 1 year, or when no longer needed, whichever is sooner.
T36 - 40 R01.00 - Curriculum Materials Used in Formal Training Courses-Current Courses, Nonrecord Sets of Current Training Materials etc; Destroy when superseded or revised.
T36 - 40 R02.01 - Curriculum Materials; Used in Formal Training Courses Substantially Revised and Discontinued Courses – Other; Curriculum Materials Used in Formal Training Courses Substantially Revised and Discontinued Courses - Other
T36 - 44 R02.00 – Training Aids Usage; Destroy 3 months after completion of training phase, provided required flying time is posted on individual flight records.
T91 - 04 R24.00 - All Job Safety Training; Retain at unit until individual goes PCS or PCA; then individual shall hand carry AF Form 55 to next assignment.
T91 - 04 R25.00 - Job Safety Training/Discharged/Separated or Retired; Destroy after one year.
Note: Among the disposition(s) cited in this field, the one with the longest retention time will be used on the system's records data

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.

AFI 36-2670, Total Force Development; and AFI 36-2650 (Maintenance Training) AFMC Sup, 2 May 2019.

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.

TSS doesn't collect information 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)*

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

Civilian government series number (example: 2210, 0391, etc.) and employee ID 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 ☒ No

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

n/a

(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 ☐ No

SSNs were removed from TSS on 8 Mar 2019.

b. What is the PII confidentiality impact level[2]? ☒ Low ☐ 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.

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.