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:

Software Maintenance Tools Suite (SMTS)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

11/03/23

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
- [x] 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
- [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.

- System Purpose: SMTS (Software Maintenance Tools Suite) is a metrics and data engineering software tool suite providing many services to the 76 Software Engineering Group. The application provides support as required by CMMI (Capability Maturity Model Integrated) and ISO 9001 mainly by relating AF charge codes to SWEG projects and tasks, thereby allowing SWEG employees to enter daily tasks which are aligned to AF Job Order Numbers. SMTS tracks direct time against projects, overheads and exceptions, allowing management to conduct agency-specific earned value management of activities, track net available funds, track material orders, and conduct financial analysis on projects by comparing actuals with planned spending allowing for a monthly accurate projection of unbilled balance. In addition, the application has extensive reporting capabilities, allowing the tracking of lessons learned by employees against various projects and topics, managing and allocating hardware or software resources, displaying organizational charts and other organizational and employee information, process technology change request data and other CMMI related data. SMTS provides a benefit to the mission by improving processes and tracking project execution in 76 SWEG, thereby improving cost, schedule as well as quality for 76 SWEG's customers. The application is web-based, allowing authenticated users to access its features via the Internet. This application was developed and is managed by the 76 SWEG group at Tinker AFB. A copy of this application is being used by Robins AFB. This system does not meet the criteria for the Internal Use Software (IUS) reporting. SMTS is hosted in the Azure Cloud One environment.
- Types of personal information collected: Employment Information, Home/Cell Phone, Mailing/Home Address, Work E-mail Address, Education Information, DoD ID Number, Emergency Contact, Names (s), Other ID Number.
The user has the choice of whether or not to enter personal information once logged in.

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 personal information is collected for emergency contact, time management, account creation, and administrative use.

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 has a choice whether or not to enter personal information once logged in. The fields are not required to be completed.
The user may delete what he/she had entered within SMTS at any time.

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

Consent banner at the start of the application states that information disclosure is voluntary and information collection is for the purpose of contacting the employee in case of an emergency only.

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 Act Statement:
THE INFORMATION ACCESSED THROUGH THIS SYSTEM IS FOR OFFICIAL USE ONLY AND MUST BE PROTECTED IN ACCORDANCE WITH THE PRIVACY ACT OF 1974.
The information you provide to the SMTS system is covered by the Privacy Act of 1974. To receive a copy of the Privacy Act Statement for the actions you enter into the system, please see your Group Tools Admin.

AUTHORITY: 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.

PRINCIPAL PURPOSES: SMTS system collects information from DOD civilians and contractors for personnel accountability and contacting listed family/friend in emergency situations.

ROUTINE USES: IIn addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a Routine Use pursuant to 5 U.S.C. 552a(b)(3) as follows:
The DoD "Blanket Routine Uses" published at the beginning of the Air Force's compilation of systems of records notices may apply to this system.
1. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

2. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

3. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

4. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

5. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

6. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

7. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

DISCLOSURE: Disclosure is voluntary; however, if the employee fails to provide the information requested, management will not be able

to contact the employee in case of an emergency.

SORN: Enterprise Identity, Credentialing, and Access Management (ICAM) Records, DoD–0015.

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.	
☐ 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
- ☒ Existing DoD Information Systems
- ☐ Other Federal Information Systems
- ☐ Databases
- ☐ Commercial Systems

Depot Maintenance Accounting and Production System (DMAPS)

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

- ☐ E-mail
- ☐ In-Person 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

- The user OPTIONALLY enters personal information on SMTS "Edit Account Info" page, once logged in to the system.

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. DAA-GRS-2019-0004-0002; N1-AFU-90-03

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

(3) Retention Instructions.

T 65 - 22 R 03.00 - Individual Attendance and Overtime (including Flexitime Sheets) -- Destroy after GAO audit or when 6 years old, whichever is sooner. See note for exception to this time period for Italian attendance and overtime records.
T 32 - 04 R 02.00 - Daily Labor Analysis and Work Status Reports -- Destroy after receipt of weekly report.
T 36 - 36 R 04.00 - Personnel Records -- Destroy after 2 years or when no longer needed, whichever is sooner.

Note 1: Among the disposition(s) cited in this field, the one with the longest retention time will be used on the system's records data.
Note 2: If one or more of the disposition(s) cited in this field have the disposition authority of "Unscheduled" and/or "Column D Disposition" with "Disposition pending", treat these records data as if they have a permanent retention and do not dispose them until the unscheduled status is updated by a National Archives and Records Administration (NARA-approved records disposition schedule, either pre-approved by a NARA General Records Schedule (GRS) or by a NARA-approved customized disposition schedule via the AF Form 525 process in AFI 33-322.
Note 3.: If one or more of the disposition(s) cited in this field have a permanent retention or "Column D Disposition" with "Retire as permanent", do *not* delete the records data, retain the data (it may be 25-30 years before the time of accessioning), and then before the time of accessioning, prepare the records

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.

5 U.S.C. 301, Departmental Regulations; Chapter 53, Pay Rates and Systems, Chapter 55, Pay Administration, Chapter 61, Hours of Work and Chapter 63, Leave; Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R Vol. 8

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.

SMTS only collects data from Federal Employees no OMB number is required.

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.