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:

Information Systems Management Tool (ISMT)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

04/07/2025

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 Information System Management Tool (ISMT) is a web-based and certified configuration and requirements management tracking and software workload management system. This system supports the entire software life cycle from requirements inception, through deployment and internal systems engineering activities. ISMT provides functional owners, program managers, developers, testers, configuration managers and end users complete visibility into requirement and deficiency traceability for both individual programs and roll-up composites of programs. Its dynamic query engine and custom report generator provide numerous options for gathering metrics and contains an integrated action tracking capability as well. ISMT is the standard management tool for the AFMC Logistics community and is also used by Air Staff Logistics Portfolio Managers and several other functional area customers. ISMT relies upon the Air Force Portal which authenticates users via their DoD CAC and PIN. Types of personal information collected: Name(s), Work E-mail, and EDIPI number. ISMT does not collect or process social security numbers.

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)*

Identification and authentication of users to the system.

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.

Users access ISMT by authenticating through the Air Force Portal. The Air Force Portal contains a DoD Warning Banner and Consent Notice that requires users to accept prior to authentication. Upon authenticating through the Air Force Portal and accessing ISMT, the system displays its own warning banner that users must accept prior to utilizing the site. The Consent Notice includes provisions that state that the data stored on the system, to include authentication and access control data, are not private and are subject to monitoring, interception, search, disclosure, and use by the U.S. Government for any authorized purpose. Access to ISMT requires that all connecting users accept the Consent Notice. Otherwise, users that deny the consent notice will not be granted access to the system.

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 access ISMT by authenticating through the Air Force Portal. The Air Force Portal contains a DoD Warning Banner and Consent Notice that requires users to accept prior to authentication. Upon authenticating through the Air Force Portal and accessing ISMT, the system displays its own warning banner that users must accept prior to utilizing the site. The Consent Notice includes provisions that state that the

data stored on the system, to include authentication and access control data, are not private and are subject to monitoring, interception, search, disclosure, and use by the U.S. Government for any authorized purpose. Access to ISMT requires that all connecting users accept the Consent Notice.

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

Users accessing the system are redirected to the Air Force Portal and are required to accept the consent notice. The consent notice contains the following provisions regarding how the system may collect, store, and process their private information: 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. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. NOTICE: There is the potential that information presented and exported from the AF Portal contains FOUO or Controlled Unclassified Information (CUI). It is the responsibility of all users to ensure information extracted from the AF Portal is appropriately marked and properly safeguarded. If you are not sure of the safeguards necessary for the information, contact your functional lead or Information Security Officer.
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.

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.	USAF - ISMT USAF - Cloud One GCDS USAF - Air Force Portal
☐ 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.	Depot Maintenance Application Consolidation II (DMAC II) Contract - Contract includes a section that requires the protection of CUI and unclassified DoD information not approved for public release on non-DoD information systems and for such information to be protected in-accordance with DoDI 8582.01, Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information, and NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations EPASS Contract - Contract includes a section for CUI and states that all CUI requires safeguarding or disseminating controls.
☐ 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

ISMT collects PII from the following DoD Information system: Air Force Portal and Cloud One Global Content Delivery System (GCDS).

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)*

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 Enterprise ICAM Records 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. N1-AFU-87-40

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

(3) Retention Instructions.

T 33 - 14 R 01.00 - System Software Case Files at the OPR for Tasked System -- Destroy 2 years after disapproval or discontinuance of system, or when no longer needed, whichever is later.
T 33 - 14 R 02.00 - System Software Case Files @ Supporting Activity not Having Prime Responsibility, Program Releases & Changes -- Destroy when superseded, obsolete, or no longer needed, whichever is later.
T 33 - 14 R 03.00 - Management Task Control -- Destroy 5 years after task closing.

Note 1: Among the dispositions cited in this field, the one with the longest retention time will be used on the system's records data.
Note 2: If any disposition cited in this field has a pending or unscheduled disposition, treat records as permanent retention until an approved NARA disposition is published.
Note 3: If any disposition cited in this field have a permanent retention, retain the records, and prepare for transfer to NARA as scheduled.

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.

Title 5, United States Code, Section 552a; DD Form 2875: Executive Order 10450; Public Law 99-474: The Computer Fraud and Abuse Act; 10 U.S.C. 2222, Defense Business Systems, 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.

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.

ISMT does not collect or process PII from members of the public.

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.