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:

Security Assistance Management Information System (SAMIS)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

09/16/24

DSCA

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
- [x] 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.

The Security Assistance Management Information System (SAMIS) is the sole Air Force System responsible for Foreign Military Sales (FMS) sustainment activities. SAMIS's role is to provide logistic capabilities for the Air Forces' Security international partners to acquire Materiel and Services to support their missions. This includes Requisition input, status processing, delivery tracking, and final billing visibility. SAMIS is a main frame based system hosted at DEC Mechanicsburg PA. The customer base is worldwide and has approximately 1000 FMS stakeholder Accounts. SAMIS is slated for replacement via the Security Cooperation Enterprise Solution that will encompass Army, Navy and Air Force functionality; however a firm sunset date is not known at this point of the modernization project.
PII being collected: names, official duty address, official duty phone number, work email address.

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, identification, and authentication to the mainframe.

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.

Employees implicitly consent to the capture and use of their PII at the time of employment. Prior to the collection of PII, users are provided appropriate Privacy Act Statement via DD Form 2875 and given an opportunity to object to any collection of PII at that time. However, if the requested information is not provided, the potential user will not receive access to the system.

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.

Users implicitly consent to the capture and specific use of their PII upon completion of DD Form 2875 for account creation and access. However, if the requested information is not provided, the potential user will not receive access to the system.

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.)*

- [x] Privacy Act Statement
- [ ] Privacy Advisory
- [ ] Not Applicable

Upon the collection of PII, individuals subject to the Privacy Act are provided appropriate Privacy Act Statements. For access, DD Form 2875, System Authorization Access Request (SAAR) is completed, and the form includes the following Privacy Act Statement: Authority:

Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. 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.

In 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:
A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records.
B. 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.
C. 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.
D. 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.
E. 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.
F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines 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.
H. 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.
I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act of 1987, as amended.
J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.
SORN: Enterprise Identity, Credential, 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)*

[x]	Within the DoD Component	Specify.	USAF
[x]	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	DISA, DSCA
[ ]	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
[ ]	State and Local Agencies	Specify.	
[x]	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.	CONTRACTORS: SierTek, JYG, and Datum for development, configuration management and Endeavor admin support. The contracts contain provisions to ensure the confidentiality and security of PII are in place to manage data risks, including language addressing the completion of orientation and annual privacy training for contractor employees. See Privacy Clauses 52.224-1, 52-224-2 and 52-224-3.
[ ]	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)*

☐ 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)*

DD form 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 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-90-03; N1-AFU-94-03

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

(3) Retention Instructions.

T 16 - 01 R 07.00; Foreign Military Sales (FMS)--Destroy 30 years after the case is closed. Record freeze on records of Foreign Military Sales to Iran (IRA) and Foreign military sales to Pakistan (PAK).
T 65 - 06 R 4.00; Foreign Military Sales (FMS) (Military Assistance)--Destroy 10 years after FY in which case was closed. Record freeze on records of Foreign Military Sales to Iran (IRA) and Foreign military sales to Pakistan (PAK).

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.

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.

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.

[X] 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.

SAMIS is covered under the OMB control number for the DD Form 2875 (0704-SAAR) as it is the only avenue for information collection for the system.
All users accessing SAMIS are bound by the restrictions as defined in the SAAR form (DD2875). SAMIS only stores names, official duty address, official duty phone number, and work email address of users (federal employees, contractors, military members, etc.) as listed on DD form 2875.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

[X]	Yes, DITPR	DITPR System Identification Number	417
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[ ]	Yes, RMF tool	RMF tool Identification Number	
[ ]	No		

If "No," explain.

ITIPS # BI0004TQ

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

[ ]	Authorization to Operate (ATO)	Date Granted:	
[X]	ATO with Conditions	Date Granted:	3/15/2023
[ ]	Denial of Authorization to Operate (DATO)	Date Granted:	
[ ]	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

[X] Yes [ ] No

If "Yes," Enter UII 000006775 If unsure, consult the component IT Budget Point of Contact to obtain the UII.

[3]Guidance on Risk Management Framework (RMF) tools (i.e., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

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.