

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:

Acquisition Career Management System (ACMS)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

11/23/20

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 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
 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 system's purpose is to retrieve data from component personnel systems and create acquisition career field related reports on Air Force (AF) members to comply with the Defense Acquisition Workforce Improvement Act (DAWIA). This action is necessary to ensure consumers, such as civilian and military members, managers, policy makers and Congress, in support of DAWIA and the Acquisition Professional Development Program (APDP), have the necessary information to make decisions regarding qualification and acquisition personnel certification. It is maintained by the AF Acquisition Training Office at Randolph AFB, TX. ACMS integrates, archives, and publishes Personally Identifiable Information (PII) data sourced from the Military Personnel Data System (MILPDS) and Defense Civilian Personnel Data System (DCPDS.) The types of personal information retrieved includes: Name(s), social security number, position/title, rank/grade, DoD ID number, employment information, work email, birth date, education, and off-duty telephone number.

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)

ACMS uses PII resident in MilPDS and DCPDS for the purpose of unambiguous identification of members. PII retrieved from IT systems is used to identify, manage, and characterize Acquisition workforce populations.

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.

ACMS does not interface with the user during initial collection. PII is retrieved through system interfaces with MilPDS, DCPDS, ACQNOW, ADLS, AWMFMIS, PMRT, and DSM.

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.

ACMS does not interface with the user during initial collection. PII is retrieved through system interfaces with MilPDS, DCPDS, ACQNOW, ADLS, AWMFMIS, PMRT, and DSM.

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

Authority: 10 U.S.C. Section 9013. Secretary of the Air Force; 10 U.S.C. Chapter 31, Enlistments; 10 U.S.C. Chapter 81, Civilian

Employees; 10 U.S.C. Chapter 87, Defense Acquisition Workforce Improvement Act; 10 U.S.C. Chapter 913, Enlistments; 10 U.S.C. Chapter 915, Appointments in the Regular Air Force; 10 U.S.C. Chapter 919, Temporary Appointments; 10 U.S.C. Chapter 921, Active Duty; 10 U.S.C. Chapter 933, Miscellaneous Rights and Benefits; 10 U.S.C. Chapter 937, Decorations and Awards; 10 U.S.C. Chapter 941, Retirement for Length of Service; 10 U.S.C. Chapter 943, Retired Grade; 10 U.S.C. Chapter 945, Computation of Retired Pay; 5 U.S.C. Chapter 12, Merit Systems Protection Board, Office of Special Counsel, and Employee Right of Action; 5 U.S.C. Chapter 14, Agency Chief Human Capital Officers; 5 U.S.C. Part III- Employees; 37 U.S.C. Pay and Allowances of the Uniformed Services; 32 U.S.C. National Guard; AFI 36-2110, Total Force Assignments; AFI 36-2406, Officer and Enlisted Evaluation Systems; AFI 36-2502, Enlisted Airman Promotion/Demotion Programs; AFI 36-2606, Reenlistment and Extension of Enlistment in the United States Air Force; AFI 36-2608, Military Personnel Records System; AFI 36-2670, Total Force Development; AFI 36-2905, Fitness Program; AFI 36-3009, Airman and Family Readiness Centers; AFI 36-3012, Military Entitlements; AFMAN 36-2664, Personnel Assessment Program; AFMAN 36-2032, Military Recruiting and Accessions; E.O. 9397 (SSN), amended by EO 13478.

Purpose: ACMS supports the implementation of Defense Acquisition Workforce Improvement Act (DAWIA) and Acquisition Professional Development Program.

Routine Uses: Information will not be released outside of DoD. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records 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 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.
- 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 any person, organization or governmental entity (e.g., local governments, first responders, American Red Cross, etc.), in order to notify them of or respond to a serious and imminent terrorist or homeland security threat or natural or manmade disaster as is necessary and relevant for the purpose of guarding against or responding to such threat or disaster.
- j. To other Federal, State and local Government/Quasi-Government Agencies when such data is required in the performance of official duties (e.g., military service and benefits determination, compensation, service member and family support, certifications, credentials, or licensing), these include but are not limited to the Office of Personnel Management, Defense Finance and Accounting Service, Social Security Administration, Selective Service Agencies, Veterans Administration, Labor Department, Red Cross, Federally Funded Research and Development Centers, National Security Agency, Federal Aviation Administration, or other military services.
- k. To military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharges, or retired from the Armed Forces, information as to last known residential or home for record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

Disclosure: Voluntary. An individual's collection of their PII in the source PDS' (MILPDS (SSN)/DCPDS) are contingent upon their employment. If information is not provided, ACMS access is denied.

AF SORN: F036 AF PC Q Personnel Data System (PDS).

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: PII is retrieved for the unambiguous identification of Acquisition workforce personnel.
 Existing DoD Information Systems: ACMS retrieves PII electronically through established and approved interfaces with MilPDS, DCPDS, ACQNOW, ADLS, AWMFMIS, PMRT, and DSM to identify, manage, and characterize Acquisition workforce populations.

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)

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://dpclid.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.

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

(3) Retention Instructions.

T33 - 42 R 08.00; Office Projects/Studies at Major Subordinate Command OPRs and Above - Destroy 20 years after completion of project/study or when no longer needed.
T36 - 32 R 09.00; Employee Training Development - Destroy when replaced by a new CEP or when no longer needed, whichever is sooner.
T36 - 19 R 19.00; USAF Personnel Plan - Destroy when superseded, obsolete, or no longer needed.

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.

10 U.S.C. Section 9013, Secretary of the Air Force; 10 U.S.C. Chapter 31, Enlistments; 10 U.S.C. Chapter 81, Civilian Employees; 10 U.S.C. Chapter 87, Defense Acquisition Workforce Improvement Act; 10 U.S.C. Chapter 913, Enlistments; 10 U.S.C. Chapter 915, Appointments in the Regular Air Force; 10 U.S.C. Chapter 919, Temporary Appointments; 10 U.S.C. Chapter 921, Active Duty; 10 U.S.C. Chapter 933, Miscellaneous Rights and Benefits; 10 U.S.C. Chapter 937, Decorations and Awards; 10 U.S.C. Chapter 941, Retirement for Length of Service; 10 U.S.C. Chapter 943, Retired Grade; 10 U.S.C. Chapter 945, Computation of Retired Pay; 5 U.S.C. Chapter 12, Merit Systems Protection Board, Office of Special Counsel, and Employee Right of Action; 5 U.S.C. Chapter 14, Agency Chief Human Capital Officers; 5 U.S.C. Part III- Employees; 37 U.S.C. Pay and Allowances of the Uniformed Services; 32 U.S.C. National Guard; AFI 36-2110, Total Force Assignments; AFI 36-2406, Officer and Enlisted Evaluation Systems; AFI 36-2502, Enlisted Airman Promotion/Demotion Programs; AFI 36-2606, Reenlistment and Extension of Enlistment in the United States Air Force; AFI 36-2608, Military Personnel Records System; AFI 36-2670, Total Force Development; AFI 36-2905, Fitness Program; AFI 36-3009, Airman and Family Readiness Centers; AFI 36-3012, Military Entitlements; AFMAN 36-2664, Personnel Assessment Program; AFMAN 36-2032, Military Recruiting and Accessions; E.O. 9397 (SSN), amended by EO 13478.

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.

ACMS does not collect information from the general public. Para 2 APPLICABILITY, b. Does not apply to: (1) Component internal information collections that do not collect information 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.