



PRIVACY IMPACT ASSESSMENT (PIA)

For the

AWACS Management System (AMS)

United States Air Force

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

Executive Order 9397 Section A2.6; AFI 11-401 Aviation Management; AFI 11-202 Aircrew Standardization/Evaluation Program

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

AWACS Management System (AMS) is an integrated database that incorporates personnel management, personnel scheduling, mission scheduling, crew scheduling, training, mobility, aircrew status, and flying currency management into a single web-hosted application. AMS delivers information to customers via web-based front end. AMS is available to some 5,700 users in the 552d Air Control Wing (552 ACW) Tinker AFB Ok and support units.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Availability of individual's information is permission based thus limiting access. Personnel that have access to this information have been authorized by their Wing/Group/Squadron Commanders.

The individual units are responsible for protecting the privacy rights of the employees affected data collected within AMS

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Other (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

Yes No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

AMS is used to schedule personnel assigned to 552d Air Control Wing (552 ACW) Tinker AFB OK and support units. The gathered privacy information is required to create the schedules, load lists, class rosters, etc.

j. 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.

AMS is used for military operations. The military (US Air Force) already provided consent when they joined the service.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Privacy Act Statement

Privacy Advisory

Other

None

Describe each applicable format.

Authority for Maintenance of the System: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 8013, Secretary of the Air Force; AFI 11-202V2 ACC Sup Aircrew Standardization/Evaluation Program; AFI 11-401 Aviation Management; ACCI 11-464 Training Records and Performance Evaluation in Formal Flying Training Programs; and E.O. 9397 (SSN).

Purpose(s): To manage and administer Air Force aviation and non-flying operations. This includes aircrew training and evaluation, flight schedule functions, flying safety and related functions needed to attain and maintain combat or mission readiness, ancillary training, scheduling functions, mobility/ deployment requirements tracking.

Disclosure Authority: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, these records contained therein, 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 apply to this system

NOTE:

Sections 1 and 2 above are 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 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

(3) How will the information be collected? Indicate all that apply.

- | | |
|---|--|
| <input type="checkbox"/> Paper Form | <input checked="" type="checkbox"/> Face-to-Face Contact |
| <input type="checkbox"/> Telephone Interview | <input type="checkbox"/> Fax |
| <input type="checkbox"/> Email | <input type="checkbox"/> Web Site |
| <input type="checkbox"/> Information Sharing - System to System | |
| <input type="checkbox"/> Other | |

If "Other," describe here.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

AMS is used to schedule personnel assigned to 552d Air Control Wing (552 ACW) Tinker AFB OK and support units. The gathered privacy information is required to create the schedules, load lists, class rosters, etc.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

AMS is used to schedule personnel assigned to 552d Air Control Wing (552 ACW) Tinker AFB OK and support units. The gathered privacy information is required to create the schedules, load lists, class rosters, etc.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

- Yes No

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

- Users Developers System Administrators Contractors
 Other

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Security Guards | <input checked="" type="checkbox"/> Cipher Locks |
| <input checked="" type="checkbox"/> Identification Badges | <input type="checkbox"/> Combination Locks |
| <input checked="" type="checkbox"/> Key Cards | <input type="checkbox"/> Closed Circuit TV (CCTV) |
| <input type="checkbox"/> Safes | <input type="checkbox"/> Other |

Tinker AFB Security Guards. AMS servers are maintained in a 24/7 manned brick building with limited access.

(2) Technical Controls. Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> User Identification | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Password | <input checked="" type="checkbox"/> Firewall |
| <input checked="" type="checkbox"/> Intrusion Detection System (IDS) | <input type="checkbox"/> Virtual Private Network (VPN) |
| <input type="checkbox"/> Encryption | <input checked="" type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input type="checkbox"/> External Certificate Authority (CA) Certificate | <input checked="" type="checkbox"/> Common Access Card (CAC) |
| <input type="checkbox"/> Other | |

If "Other," specify here.

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits**
- Regular Monitoring of Users' Security Practices**
- Methods to Ensure Only Authorized Personnel Access to PII**
- Encryption of Backups Containing Sensitive Data**
- Backups Secured Off-site**
- Other**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

Yes. Indicate the certification and accreditation status:

- | | | | |
|-------------------------------------|--|----------------------|-----------|
| <input checked="" type="checkbox"/> | Authorization to Operate (ATO) | Date Granted: | 1 July 08 |
| <input type="checkbox"/> | Interim Authorization to Operate (IATO) | Date Granted: | |
| <input type="checkbox"/> | Denial of Authorization to Operate (DATO) | Date Granted: | |
| <input type="checkbox"/> | Interim Authorization to Test (IATT) | Date Granted: | |

No, this DoD information system does not require certification and accreditation.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

AMS is in the fully operational/sustainment phase.
AMS Access Control

A. AMS provides detailed and specific access levels and permissions to ensure that only authorized users have access to read and or write information, or perform other operations with the system. Access to AMS will be granted using the Common Access Card (CAC) or username/password security model and from .MIL address. Access to specific modules are managed through the Account Administration module.

B. A combination of physical, personnel, and system-enforced security mechanisms control access to AMS. The Least Privilege Principle is implemented, which means that users will be given privileges, capabilities, and roles associated with their user-identifications (user-ids) that have the least amount of "power" or privilege that still +

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

AMS Access Control

A. AMS provides detailed and specific access levels and permissions to ensure that only authorized users have access to read and or write information, or perform other operations with the system. Access to AMS will be granted using the Common Access Card (CAC) or username/password security model and from .MIL address. Access to specific modules are managed through the Account Administration module.

B. A combination of physical, personnel, and system-enforced security mechanisms control access to AMS. The Least Privilege Principle is implemented, which means that users will be given privileges, capabilities, and roles associated with their user-identifications (user-ids) that have the least amount of "power" or privilege that still enables them to do their jobs. As with functional users, explicit controls limit access capabilities associated with System Administrator or other Trusted Official privileged roles or functions.

C. AMS security features include techniques that limit or otherwise restrict access to the Trusted Computer Base (TCB) or its capabilities to specified users or user groups. Specifically assigned user-ids and password sequences are used to control access to AMS, consistent with privileges and capabilities to be granted.

D. All users accessing AMS shall be explicitly granted appropriate permissions and privileges according to their mission task requirements. Consequently, no person by virtue of rank or position only has the right to access or use AMS. All accesses, whether procedural or system-enforced, are adjudicated based on each person's authorized "need-to-know."

E. AMS servers are maintained in a 24/7 manned brick building.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

N/A