



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Army Workload and Performance System (AWPS)

AMC - JMC - U.S. Army Joint Munitions Command/Deputy Under Secretary of the Army  
(DUSA)

### 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.

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, Chapter 5, Leave; E.O. 9397 (SSN), as amended. 5 U.S.C. 7201, Antidiscrimination Policy; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness;

**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.

To provide Workload and Performance data on civilian, military, contractor and foreign nationals for Department of Defense (DoD) Components and the Department of Navy located worldwide. This system will gather or capture time and attendance, labor and production data for input to Army Workload and Performance System (AWPS) Work Mapping Tool (WMT), Time Collection Tool (TCT), Performance Measurement and Control (PMC) and Strategic Planning and Forecasting (SPF) modules. It will also provide the user a single, consolidated input method for reporting both time and attendance and labor information to be used in Earned Value Management (EVM) toolsets inside of AWPS.

AWPS aids managers in determining the number and type of resources necessary and available to complete scheduled work. AWPS loads work force, workload, and timecard data from existing Department of the Army personnel systems, and then replicates the data to a central repository. The data acquired from these sources is used in the AWPS system's background processing to derive an aggregate number of employee and supervisor hours worked on projects. This data is essential for forecasting workload and resource requirements.

As an operational system, the AWPS user community and the development team use best practices, adhere to Department of Defense (DoD) and Department of the Army (DA) security requirements, and are committed to protecting personally identifiable information (PII). The type of PII collected is personal and employment information.

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

a) The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.).

b) All systems are vulnerable to "insider threats". The Information Assurance Manager (IAM) and Information Assurance Officers (IAO) along with the responsible Commands Information Assurance/Security personnel are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. AWPS has defined criteria to identify who should have access to the information resident in the AWPS system. These individuals are required have gone through extensive background and employment investigations.

c) The residual privacy risks regarding the collection, use, and sharing of PII is LOW. AWPS consolidates, improves and accelerates existing processes. Extraneous PII is not collected and, by reducing the number of redundant systems and copies of PII, over-all privacy risks are reduced.

d) Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Physical and electronic access are limited to persons responsible for servicing and authorized to use the system.

e) AWPS routinely processes and stores "Controlled Unclassified Information", which includes Privacy data, and is exempted from public disclosure by the Freedom of Information Act, Exemption 3 and by provisions of Department of Defense (DoD) Directive 5230.25. Privacy issues have been addressed during the system development life cycle, and protections have been integrated to protect sensitive information, including Privacy data.

**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.

DUSA, AAG, AMC, JMC, HQDA, ANC, OAA, USAR

**Other DoD Components.**

Specify. Navy, Marines (HRSC Command and their components) and National Guard Bureau (CA-ARNG) and their major commands and components.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

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

Specify. Booz Allen Hamilton Inc. under a multiple year contract WP52P1J-08-3025 is the prime contractor. Contractors are required yearly to participate in the following Privacy Training which is approved by The Chief Privacy Officer of the Navy CIO Office: Training is located at the following link; [http://iase.disa.mil/eta/pii/pii\\_module/pii\\_module/index.html](http://iase.disa.mil/eta/pii/pii_module/pii_module/index.html).

**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.

a) In cases where AWPS collects information from other systems, those systems already have offered individuals the option to object to the collection of information about themselves, or to consent to such collection.

b) Users entering into AWPS have the opportunity to decline the "use of data stored" in AWPS for authorized purposes by pressing the "Decline" button which will end their session to AWPS.

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

**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.

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

The individual does not control the specific uses of the PII data once collected into the AWPS system. PII is used to link data sets together from different data sources before being de-identified for use in other AWPS modules.

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

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> <b>Privacy Act Statement</b> | <input type="checkbox"/> <b>Privacy Advisory</b> |
| <input type="checkbox"/> <b>Other</b>                            | <input type="checkbox"/> <b>None</b>             |

Describe each applicable format.

This is the warning banner that is displayed upon each login to the user.

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- 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.
- 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.

PRIVACY ACT WARNING

This statement serves to inform you of the purpose for collecting personal information required by the Army Workload and Performance System (AWPS) and how it will be used.

AUTHORITY: 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, Chapter 5, Leave; E.O. 9397 (SSN), as amended. 5 U.S.C. 7201, Antidiscrimination Policy; 10 U.S.C. 136, Under Secretary