



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Installation Support Modules (ISM)

Department of Army/Program Executive Office (PEO) Enterprise Information System (EIS)

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 172 (DA 76239)
- 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.

The authority for the Installation Support Modules system to collect information is derived from: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Instruction 1322.25, Voluntary Education Programs; DoD Instruction 1336.01, Certificate of Release or Discharge from Active Duty (DD Form 214/215 Series); Army Regulation 735-5, Policies and Procedures for Property Accountability; and Executive Order 9397 (SSN), as amended.

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.

The Installation Support Modules system is an automated system that imports and exports personally identifiable information on United States Army Soldiers from and to external sources to provide the Army a capability manage administrative personnel and logistical functions at the Installation level. ISM provides Installation Commanders and Staffs with an automated information system (AIS) that assists in the accomplishment of day-to-day administrative tasks in the areas of soldier In/Out-processing, Transition Processing, Personnel Locator, Education Management and management of Organizational Clothing and Individual Equipment. It provides timely and accurate information necessary to facilitate installation management and assists in the obtaining of soldier readiness during periods of deployment and mobilization. The system does not create or derive new PII data about individuals, it is collected on Soldiers by the Installation Support Modules system from the Army's eMILPO system and includes everything about an individual.

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

All systems, to include the Installation Support Modules system, have threats that seek to exploit and cause harm to the information contained in the system. The types of threats include human intentional - human unintentional - structural - and natural. Therefore, risks associated with the PII data contained in the ISM system fall into the categories mentioned above. Due to the level of safeguarding associated with the ISM system, the risk to individuals' privacy is minimal. Safeguarding controls include physical, administrative and technical as found in Section III. Additionally, the ISM system is DIACAP compliant.

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. All Army components and major commands which includes Active Duty, Army Inspectors General, Army Secretariat and Army Staff Principals, Army Audit Agency, Criminal Investigation Command, INSCOM, Army Human Resources Command, and Army Materiel Command, Installation Management Command, U.S. Army Reserve Command and the Provost Marshall General.

Other DoD Components.

Specify. Defense Criminal Investigative Service, Defense Finance and Accounting Service, US Medical Command, Defense Manpower Data Center, and National Guard Bureau.

Other Federal Agencies.

Specify. Department of Veterans Affairs, Department of Labor,

State and Local Agencies.

Specify. State Directors of Veterans Affairs

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

Specify.

The ISM software developer is SRA, International located in Fairfax, VA. Specific language in the contract that addresses PII follows:
Performance of this effort may require the contractor to access and use data and information proprietary to a Government agency or Government contractor which is of such a nature that its dissemination or use, other than in the performance of this effort, would be adverse to the interests of the Government or others. Identification and handling of Personally Identifiable Information (PII) is critical to ISM and RFMSS. Executive Office of the President, Office of Management and Budget (OMB), Memorandum (M-06-19), was sent to the Chief Information Officers on 12 July 2006 requiring that all incidents involving PII be reported to the US-CERT within one hour of discovery. The Army also requires notification of the Army's Freedom of Information Act (FOIA) and Privacy Act Office within 24 hours, and affected individuals within 10 working days of an incident. Contractor shall ensure that no PII is stored on contractor equipment, nor at contractor facilities. Contractor shall ensure that all personnel are trained on proper handling of PII to include reporting of incidents.

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.

Selected contractor personnel whose PII data is not obtained from another system can object to furnishing PII data at the time they are interviewed by Central Issue Facility personnel. If an individual objects to providing PII information, he/she will not be issued Organizational Clothing and Individual Equipment.

(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.

Selected contractor personnel whose PII data is not obtained from another system can consent to furnishing PII data at the time they are interviewed by Central Issue Facility personnel.

(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.

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

Describe each applicable format.

PRIVACY ACT STATEMENT
Installation Support Modules

AUTHORITY: The legal authority for recording Personal Identifiable Information in the Installation Support Modules system is 10 USC 3013 in overall Secretary of the Army authority, and EO 9397 which authorizes the use of Social Security Numbers.

PRINCIPAL PURPOSE: Personal Identifiable Information is used by the Army's Installation Support Modules Central Issue Facility application to record information about an individual who has requested Organizational Clothing and Individual Equipment to allow him/her to perform a task or duty for the United States Army that requires the clothing or equipment.

ROUTINE USE(S): The Personal Identifiable Information will be used on hand receipts produced by the Installation Support Modules system to record items of Organizational Clothing and Individual Equipment issued to Department of Defense and non-Department of Defense personnel who are performing a task of duty for the United States Army requiring the equipment. The Personal Identifiable Information furnished at the time of equipment issue will be released only to Department of Defense personnel who have a need to know and will not be released or disclosed to anyone outside of the Department of Defense.

DISCLOSURE: Disclosure of Personal Identifiable Information is Voluntary; however, failure to provide required information will result in disapproval of your request to be issued Organizational Clothing and Individual Equipment.

THIS PRIVACY ACT STATEMENT WILL BE PROVIDED TO NON-US ARMY PERSONNEL PRIOR TO ISSUING ORGANIZATIONAL CLOTHING AND INDIVIDUAL EQUIPMENT.

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.