



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

International Affairs Personnel Initiatives Database (IAPID)

Defense Security Cooperation Agency/Defense Institute of Security Assistance Mgt.

### **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.

1) 10 U.S.C. § 134, Under Secretary of Defense for Policy

2) DoD Directive 5105.65, Defense Security Cooperation Agency

**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.

IAPID is a single central facility with the Department of Defense (DoD) that maintains and verifies information provided by individuals seeking International Affairs certification based on their current experience and training. IAPID is designed to standardize certification and career development guidelines. Information Type: Full Name; Email Address; Home/Work Mailing Address, telephone and fax numbers; Job and Education Information: Status (i.e., Civilian or Military), Major Command and Mailing Address, Organization, Office Symbol/Code, Job Title, Job Function, Grade/Rank, Job Series, Military Specialty, Start Date, Total Months in International Affairs related Work, Billet Information, Current Certification Level, Highest Education Completed, and Field of Study; Supervisor Information: First and Last Name, Email Address, Organization, Office Symbol, Work Phone and Fax Number.

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

The privacy risk would be the disclosure of the PII collected to an unauthorized source. To safeguard privacy, the records are electronically maintained in controlled areas accessible only to authorized personnel. Access to personal information is further restricted by the use of user IDs and passwords. Physical entry is restricted by locks, security personnel and administrative procedures.

**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.

The use of this database is strictly voluntary and utilized to track accomplishments and documentation of certification at one of three levels. All data is entered by the individual with the exception of certification level awarded which is entered by the component (MILDEP/Agency) administrator.

(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.

By virtue of entering the information and the supervisor's e-mail, the individual authorizes review and verification of the data entered into the system.

(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.

- 1) The Privacy Act Statement outlines the authority for collection, purpose, routine use and disclosure: voluntary.
- 2) Security Notices and Disclaimers

**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.**

**SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW**

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

- Name  Other Names Used  Social Security Number (SSN)
- Truncated SSN  Driver's License  Other ID Number
- Citizenship  Legal Status  Gender
- Race/Ethnicity  Birth Date  Place of Birth
- Personal Cell Telephone Number  Home Telephone Number  Personal Email Address
- Mailing/Home Address  Religious Preference  Security Clearance
- Mother's Maiden Name  Mother's Middle Name  Spouse Information
- Marital Status  Biometrics  Child Information
- Financial Information  Medical Information  Disability Information
- Law Enforcement Information  Employment Information  Military Records
- Emergency Contact  Education Information  Other

If "Other," specify or explain any PII grouping selected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

The source of the PII collected is from the individual user with verification of data by the respective supervisor from either records or personal knowledge.

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

- |   |   |
|---|---|
| <input type="checkbox"/> Paper Form                             | <input type="checkbox"/> Face-to-Face Contact |
| <input type="checkbox"/> Telephone Interview                    | <input type="checkbox"/> Fax                  |
| <input type="checkbox"/> Email                                  | <input checked="" 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)?**

IAPID is a single central facility with the Department of Defense (DoD) that maintains and verifies information provided by individuals seeking International Affairs certification based on their current experience and training. IAPID is designed to standardize certification and career development guidelines, which provide DoD the opportunity to enhance and develop personnel with the knowledge, skills and abilities required to support International Affairs in the 21st century from entry-level personnel to senior leadership.

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

To maintain and verify information provided by individuals seeking International Affairs certification based on their current experience and training. IAPID is designed to standardize certification and career development guidelines, which provide DoD the opportunity to enhance and develop personnel with the knowledge, skills and abilities required to support International Affairs in the 21st century from entry-level personnel to senior leadership.

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

The PII will be secured by user and administrator IDs and passwords.

**(2) Technical Controls.** Indicate all that apply.

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

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 type="checkbox"/>            | <b>Authorization to Operate (ATO)</b>            | <b>Date Granted:</b> | <input type="text"/> |
| <input checked="" type="checkbox"/> | <b>Interim Authorization to Operate (IATO)</b>   | <b>Date Granted:</b> | 23 November 2009     |
| <input type="checkbox"/>            | <b>Denial of Authorization to Operate (DATO)</b> | <b>Date Granted:</b> | <input type="text"/> |
| <input type="checkbox"/>            | <b>Interim Authorization to Test (IATT)</b>      | <b>Date Granted:</b> | <input type="text"/> |

**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?**

Data entry is made by the individual only after registering as a user and establishing a password. Records are electronically maintained in controlled areas accessible only to authorized personnel. Access to personal information is further restricted by the use of user IDs and passwords. Physical entry restricted by the locks, security personnel and administrative procedures. Access to information is based on designated supervisory access (provided by the user) utilizing DoD e-mail requiring a CAC. Administrator access is limited to specific administrator ID and passwords.

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

Data entry is made by the individual only after registering as a user and establishing a password. Records are electronically maintained in controlled areas accessible only to authorized personnel. Access to personal information is further restricted by the use of user ids and passwords. Physical entry restricted by the locks, security personnel and administrative procedures. Access to information is based on designated supervisory access (provided by the user) utilizing DoD e-mail requiring a CAC. Administrator access is limited to specific administrator ID and passwords.

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

N/A