



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Computer/Electronic Accommodations Program (CAP) Database

Department of Defense Human Resources Activity

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.

10 U.S.C. 1582, Assistive Technology, Assistive Technology Devices, and Assistive Technology Services; 29 U.S.C. 794d, Electronic and Information Technology; 42 U.S.C. Chapter 126, Equal Opportunity For Individuals With Disabilities; and DoD Instruction 6025.22, Assistive Technology (AT) for Wounded Service Members.

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 administer the Computer/Electronic Accommodations Program (CAP), a centrally funded program that provides assistive (computer/electronic) technology solutions to individuals with hearing, visual, dexterity, cognitive, and/or communications impairments in the form of an accessible work environment. The system documents and tracks provided computer/electronic accommodations. The CAP Database may also be used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness and conducting research.

The CAP Database collects individual's full name; prior assistive technology solutions provided to the individual; work email, work address and work telephone number; federal agency; computer/electronic accommodations program (CAP) request number; disability data; verification of disability; history of accommodations being sought, and their disposition, and other documentation used in support of the request for an assistive technology solution. Product and vendor contact information includes vendor name and address, vendor alias, phone number, fax number, email address, web address, order submission preference, orders, invoices, declination, and cancellation data for the product and identification of vendors, vendor products used, and product costs.

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

The potential privacy risk regarding the collection of this data is that it may be inappropriately shared/used. Data confidentiality and integrity is maintained by limiting CAP Database staff access to certain application features and functions based on the permissions granted by the CAP Database Administrator (System Administrator) when a user account is requested and established.

The security measures adopted by the system do not pose any privacy risks. These security safeguards ensure confidentiality of sensitive data by granting access to the application and data only after positive identification and authentication of the CAP staff.

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.

68 Federal partner agencies participating in the Computer/Electronic Accommodations Program for purposes of providing information as necessary to permit each agency to carry out its responsibilities under the program.

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.

Vendors will be provided with address and contact information necessary to provide products and services.

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 individual voluntarily seeks computer/assistance accommodations from this program. Participation is not mandatory. However, if needed information is not provided the individual may not receive the most appropriate accommodation for their disability or may be considered ineligible for any CAP services.

(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.

Collected information may be disclosed to Federal Government agencies participating in CAP as necessary to permit the agency to carry out its responsibilities under the program. Information may be provided to commercial vendors to permit the vendor to identify and provide assistive technology solutions for individuals

with disabilities.

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.

A Privacy Act Statement is published on the website prior to any data entry fields:

Privacy Act Statement
This statement serves to inform you of the purpose for collecting personal information required by the Computer/Electronic Accommodations Program (CAP) Database and how it will be used.

Authority
10 U.S.C. 1582, Assistive Technology, Assistive Technology Devices, and Assistive Technology Services; 29 U.S.C. 794d, Electronic and Information Technology; 42 U.S.C. Chapter 126, Equal Opportunity For Individuals With Disabilities; and DoD Instruction 6025.22, Assistive Technology (AT) for Wounded Service Members.

Purpose
To administer a centrally funded program that provides assistive (computer/electronic) technology solutions to individuals with hearing, visual, dexterity, cognitive, and/or communications impairments in the form of an accessible work environment.

Routine Uses
Collected information may be disclosed to Federal Government agencies participating in CAP as necessary to permit the agency to carry out its responsibilities under the program. Information may be provided to commercial vendors to permit the vendor to identify and provide assistive technology solutions for individuals with disabilities. Information may also be used and disclosed in accordance with 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, which incorporates the DoD "Blanket Routine Uses" published at: <http://dpcllo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx>.

Disclosure
Voluntary. However, failure to provide the requested information may result in you being considered ineligible for any CAP services.

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.