



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Computer/Electronic Accommodations Program (CAP) Portal

TRICARE Management Activity (TMA)

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.

The CAP Portal is a Government-off-the-Shelf (GOTS) product designed for the Office of the Chief Information Officer (OCIO) Program Office and CAP to support the program in providing assistive technology accommodations and services to persons with disabilities at the DoD and other Federal agencies and wounded Service members in Military Treatment Facilities (MTF), at no cost to the requesting organization.

CAP Portal is used primarily to process DoD and other government agencies requests for hardware, software, technical services, and other miscellaneous services. CAP Portal also processes information pertaining to tracking acquisitions, events, and outreach and training; such as proposals, presentations, ads, costing data, inventory, booth materials, assistive technology, and other key elements to CAP Portal's outreach and acquisition efforts. The CAP Portal allows the CAP Portal staff to report and make financial forecasts with the data that is contained within the CAP Portal system.

The CAP Portal consists of:

- CAP Acquisitions Database
- CAP Content Management System
- CAP Reporting
- CAP Marketing Database

The CAP Portal is a marketing database that tracks the number of events CAP staff attends and the materials provided at those events. CAP provides assistive technology solutions to individuals with hearing, visual, dexterity, cognitive, and/or communications impairments. The system can identify the computer/ electronic accommodations being provided and track all such accommodations for DoD as well as 68 partner agencies.

CAP Portal collects the names, disability information, work mailing address, telecommunications numbers (work phone numbers and work e-mail addresses) from each of our DoD and Federal customers to ensure their accommodation is being delivered to the correct person. Fewer than one percent of these customers may provide their home contact information if they telework as a reasonable form of accommodation. It does NOT collect social security numbers, birth date, gender, race or other personal identifying information.

Individuals requesting accommodations through CAP via the CAP Web site, fax, mail and/or e-mail will willingly provide their names, disability information, work mailing address, telecommunications numbers, and work e-mail addresses to CAP. CAP will use this information when reviewing, approving, and purchasing the appropriate and reasonable accommodation per the individual's request(s).

The CAP Portal is owned by TRICARE Management Activity (TMA) and operated by CAP.

System contact information:

Computer/Electronic Accommodations Program (CAP) Portal
TMA CAP Program Manager
5109 Leesburg Pike, Suite 504, Falls Church, VA 22041
(703) 681-3976

A full PIA was previously submitted for the CAP Portal in January 2007; signature date for TMA CIO is 1/24/2007.

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

The system collects names, disability information, and work related contact information from each of our DoD and Federal customers. 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 Portal staff access to certain

application features and functions based on the permissions granted by the CAP Portal 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 the 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.

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.

CAP Portal customers have an opportunity to update and change any information provided to CAP by submitting their updated information on a new CAP Request Form. CAP customers also will have the ability to update their information by calling or e-mailing CAP on an as-needed basis.

Individuals are given the opportunity to review their name, disability information, and work related contact information and make any necessary changes before they voluntarily submit their CAP request form on the CAP Website or through their fax machine.

(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.

CAP Portal customers have an opportunity to update and change any information provided to CAP by submitting their updated information on a new CAP Request Form. CAP customers also have the ability to update their information by calling or e-mailing CAP on an as-needed basis.

(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.	<p>A Privacy Act statement is posted on the website as follows:</p> <p>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.</p> <p>Purpose: To collect information from an individual in order to determine whether that individuals qualifies for the Computer/Electronic Accommodations Program (CAP) and what assistive technology is appropriate for that individual.</p> <p>Routine Uses: Collected information may be disclosed to Federal Government agencies participating in CAP as necessary to permit the agency to carry out is 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</p>
----------------------------------	---

incorporates the DoD "Blanket Routine Uses" published at: http://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.html

Disclosure: Voluntary. However, failure to provide the requested information may result in your 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.