

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

DoD Credentialing Program for Prevention Personnel (D-CPPP)

2. DOD COMPONENT NAME:

Under Secretary of Defense for Personnel and Readiness

3. PIA APPROVAL DATE:

06/11/24

Office of Force Resiliency, Violence Prevention Cell

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

- From members of the general public From Federal employees
- from both members of the general public and Federal employees Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one.)

- New DoD Information System New Electronic Collection
- Existing DoD Information System Existing Electronic Collection
- Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Department of Defense (DoD) maintains a credential for the Integrated Primary Prevention Workforce (IPPW), the DoD Credentialing Program for Prevention Personnel (D-CPPP). All IPPW members must be Military or Department of Defense (DoD) civilian employees and must hold this D-CPPP Certification to perform CPPP duties. There are four (4) Certification levels for D-CPPP: Level II-Prevention Support, Level III-Prevention Specialist, Level IV-Prevention Lead, Level V-Prevention Program Manager. To obtain the credential, IPPW members must meet training, education, suitability, and performance standards. All applicants must submit a signed application, current resume or curriculum vitae (CV), position description, and their DoDSPARX Level 1 & 2 Training Certificates.

Information collected includes: Applicant's first name, middle name, and last name; DODID; position; Service/DoD affiliation and status; grade/rank; installation/command; Commanding Officer/Supervisor name, title, and work email: applicant work email address and telephone number; official military address(street, city, state, ZIP code, country); position level (Level II, III, IV, or V); certificates of training; date of application; verification of past experience through resume/CV (position, dates, hours)

This information may also be used to review, process, and report on program and workforce statuses.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

Identification, verification, certification, qualification, analysis

e. Do individuals have the opportunity to object to the collection of their PII? Yes No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Applicants may object to the collection of their PII by not submitting their PII on the required forms. However, they may not be considered qualified to perform their duties if they do not submit the information required to become credentialed.

f. 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.

Applicants cannot give or withhold their consent to specific uses or their PII once submitted, however, PII will only be used for the purpose stated above and within the Privacy Act Statement.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

- Privacy Act Statement Privacy Advisory Not Applicable

DoD Credentialing Program for Prevention Personnel (D-CPPP)

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Instruction (DoDI) 6400.11, DoD Integrated Primary Prevention Policy for Prevention Workforce and Leaders; and DoDI 6400.09, DoD Policy on Integrated Primary Prevention of Self-Directed Harm and Prohibited Abuse and Harm.

PURPOSE: The information provided on this form will be used to review and process applications for the Department of Defense Credentialing Program for Prevention Personnel (D-CPPP).

ROUTINE USES: Disclosure of records are generally permitted under 5 U.S.C. 522a(b) of the Privacy Act of 1974, as amended. To contractors responsible for performing or working on contracts for the DoD when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure that apply to DoD officers and employees.

Additional routine uses are listed in the applicable System of Records Notice, DHRA 10 DoD at: <https://dpcl.d.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DHRA-10-DoD.pdf>

DISCLOSURE: Voluntary. However, if you are a member of the Integrated Primary Prevention Workforce and do not complete this form to become credentialed, you may be disqualified from the position.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component?

(Check all that apply)

- | | | |
|---|----------|---|
| <input type="checkbox"/> Within the DoD Component | Specify. | <input type="text"/> |
| <input checked="" type="checkbox"/> Other DoD Components (i.e. Army, Navy, Air Force) | Specify. | USA, USN, USMC, DON, DAF, NGB |
| <input checked="" type="checkbox"/> Other Federal Agencies (i.e. Veteran's Affairs, Energy, State) | Specify. | USCG |
| <input type="checkbox"/> State and Local Agencies | Specify. | <input type="text"/> |
| <input checked="" type="checkbox"/> Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.) | Specify. | Chenega Analytic Business Solutions LLC
10505 Furnace Rd, STE 205
Lorton, VA 22079-2636 |
| <input checked="" type="checkbox"/> Other (e.g., commercial providers, colleges). | Specify. | RAND National Defense Research Institute (FFRDC) |

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Individuals | <input type="checkbox"/> Databases |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems | |

Component personnel systems

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

- | | |
|---|---|
| <input checked="" type="checkbox"/> E-mail | <input checked="" type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> In-Person Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

DD Forms 3190 and 3191

k. 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 must be consistent.

- Yes No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.defense.gov/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

I. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Cut off annually. Destroy 3 years after cutoff.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
- (2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
 - (b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Instruction (DoDI) 6400.11, DoD Integrated Primary Prevention Policy for Prevention Workforce and Leaders; and DoDI 6400.09, DoD Policy on Integrated Primary Prevention of Self-Directed Harm and Prohibited Abuse and Harm.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 No Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
- (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."
- (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

The credentialing program does not collect information on members of the public.