

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:

Certification Management System (CMS)

2. DOD COMPONENT NAME:

National Geospatial-Intelligence Agency

3. PIA APPROVAL DATE:

11/22/19

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- | | |
|--|--|
| <input type="checkbox"/> From members of the general public | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

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

- | | |
|--|---|
| <input checked="" type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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 Certification Management System (CMS), managed by the GEOINT Professional Certification Program Management Office (GPC-PMO), is a web-based, password-protected environment. The CMS is used by US and Allied civilian, military, and contractor personnel, as well as former members of these groups (through retirement and career changes) who have earned or are seeking to earn GEOINT Professional Certification credentials. The CMS enables users to manage and maintain their credentials and allows the Global GEOINT Enterprise to manage and monitor their certified affiliates, which include all government employees with a need for GEOINT certification.

User permission levels will include user and privileged users. Users will have ability to add and edit their own information. Privileged users will be limited to GPC PMO personnel with a need-to-know and to system developers. View permissions will be available for a limited number of component representatives.

The personal information collected is the first and last name, middle initial, email addresses (personal and business), organization level affiliation (NGA, Army, Air Force, etc.), business phone number, and supervisor name and email address. Users will input activities completed to satisfy Professional Development Unit (PDU) requirements. All information is maintained at an UNCLASSIFIED//FOUO classification level or lower.

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)

PII is collected to enable the GPC-PMO to effectively update accounts through data matching and identification, mission-related use for the Global GEOINT Enterprise through managing and monitoring their certified affiliates, and identification for users to access and update their own data

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.

The minimal PII collected and used in the Certification Management System (CMS) is necessary for identification of and individual with his/her exam results and credentials. The only means by which candidates will be able to view results or maintain credentials is through the CMS.

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.

The GPC PMO will create accounts for certified users; this will be the means of receiving exam results and certification maintenance.

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

PERSONAL DATA - PRIVACY ACT OF 1974 Information collected by, contained within, or extracted from CMS may contain Personally Identifiable Information (PII), and is for official use only. Should you receive any PII in error, please advise the sender immediately and promptly discard such information, in addition to immediately notifying the NGA Privacy and Civil Liberties Division (MOCP) of such unauthorized PII receipt. All unintended recipients are hereby advised that any use, inclusive of redistribution, copying or other form of unauthorized actions, is strictly prohibited. Please note that unauthorized dissemination or use of PII is a violation of Federal law. Individuals determined to be in violation may be subject to fines, disciplinary actions or both in accordance with applicable Federal law and/or policy. (P.L. 93-579)

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

- Within the DoD Component Specify.
- Other DoD Components Specify.
- Other Federal Agencies Specify.
- State and Local Agencies Specify.
- 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.
- Other (e.g., commercial providers, colleges). Specify.

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

- Individuals Databases
- Existing DoD Information Systems Commercial Systems
- Other Federal Information Systems

The database is a GPC PMO Access database of candidates from which data will be pulled.

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

- E-mail Official Form (Enter Form Number(s) in the box below)
- Face-to-Face Contact Paper
- Fax Telephone Interview
- Information Sharing - System to System Website/E-Form
- Other (If Other, enter the information in the box below)

Information will be collected on official GPC exam answer sheets. If an email address or name is updated, it will be provided through email, in person, or over the phone.

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.

Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. Destroy when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later. Destroy immediately after copying to a record-keeping system or otherwise preserving, but longer retention is authorized if required for business use.

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.

Title 10 United States Code 442, Title 50 United States Code 3045 and Department of Defense Manual 3305.10.

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.

Per Department of Defense Manual 8910.01 "DOD Information Collection Manual: Procedures for DOD Public Information Collections.- V2-para 8 (B) item # 7, Examinations designed to test the aptitude, abilities, or knowledge of the persons tested and the collection of information for identification or classification in connection with such examination is not considered Public Information Collections.