

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:

(U) Intelligence Community Badge System (ICBS)

2. DOD COMPONENT NAME:

National Geospatial-Intelligence Agency

3. PIA APPROVAL DATE:

11/18/19

Industrial and Physical Security (SISI)

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 type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input type="checkbox"/> Existing DoD Information System | <input checked="" 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.

(U) The ICBS provides seamless entry control point access at participating Intelligence Community (IC) facilities. Individual IC agencies maintain complete control of badge operations within their respective agency. IC personnel badge data can be shared through ICBS over a secure network allowing access to enter participating agencies at entry control points using existing badge and personal identification number (PIN). ICBS collects and stores personally identifiable information (PII) such as name, social security number, PIN, organization, and other uniquely identifying data elements to validate access.

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)

(U) The ICBS interface specifications are documented in the ICBS Specification published by NGA, which defines the format for all ICBS records. This record format includes numerous mandatory fields including First Name, Last Name, SSN, Badge ID (LCN), PIN, Badge Creation Date, Badge Expiration Date, Owning Agency, etc. SSN is one of the key mandatory fields for participation in the ICBS, as it is the primary field used for identification and validation of individuals entering IC facilities.

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.

(U) NGA operations require all individuals to be issued an IC badge or Common Access Card (CAC) as part of their employment. Non consent would result in denial of access to the IC facilities and information systems.

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.

(U) Any individual issued a IC badge or Common Access Card (CAC) is advised of their Privacy Act Statement (PAS) and their rights and responsibilities prior to issuing badges for facility access.

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.)

- | | | |
|--|---|--|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory | <input checked="" type="checkbox"/> Not Applicable |
|--|---|--|

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.

National Geospatial-Intelligence Agency, Industrial and Physical Security (SISI)

Other DoD Components

Specify.

Shared across the Department of Defense/Intelligence Community Agencies to include National Security Agency (NSA); Defense Intelligence Agency (DIA); National Reconnaissance Office (NRO); Office of Naval Intelligence (ONI); Marine Corps Intelligence Activity (MCIA); U.S. Army Intelligence and Security Command (INSCOM); Headquarters U.S. Department of the Air Force (HQ USAF); U.S. Naval Security Group Command (NSG); and U.S. Coast Guard (USCG).

Other Federal Agencies

Specify.

All non- Department of Defense (DoD) components designated as Intelligence Community (IC) Agencies to include Central Intelligence Agency (CIA); Department of Energy (DoE); Department of State (DOS/INR); Department of Homeland Security (DHS); Department of Treasury; Drug Enforcement Administration (DEA); Federal Bureau of Investigation (FBI); and Office of the Director of National Intelligence (DNI).

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

National Security Agency (NSA) - the Executive Agent for all Intelligence Community (IC) partners that participate in using the ICBS and SMS systems.

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)

DoD Form 2875 - paper forms for establishing user computer accounts and access controls and permissions on IC systems that are stored by the NGA Security Office (SIS).

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 NGA003 - Agency Enterprise Workforce

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.

GRS 3.2-031 - Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. GRS 3.2-041 - Destroy when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later. GRS 5.1-020 - 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 50 United States Code §402a,
- Executive Order 9397, 10450 & 12968,
- Federal Register 5 CFR part 732, part 736,
- Federal Register 32 CFR part 147
- Title 5 United States Code 301, & Title 5 United States Code 7532
- Dept of Defense Directive 5105.60, & Dept of Defense Directive 5200.2-R

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 Dept of Defense Manual 8910.01 "DOD Information Collection Manual: Procedures for DoD Public Information Collections." -Vol 2, Enclosure 3, Section 8.a (4), which is the conduct of Intelligence Activities as described in Executive Order 12333 does not require an OMB control number.