



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enterprise Business Application Suite (EBAS)
--

Strategic Programs and Innovation Office, Mission Support Team
--

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

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

OPM GOVT-1, DPR34DoD, CIG-09

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.

The authority to collect information in this system derives from:

Executive Order 10450, "Security requirements for Government Employees", April 27, 1953
DoD 5200.2-R, "Personnel Security Program", January 1, 1987

U.S. Code:

5 U.S.C. § 301, Regulations for the Government of the Department;
44 U.S.C. 3101 Records Management by Federal Agencies.
Executive Order 10450

DoD Directives:

DoD Directive 5015.2, "DOD Records Management Program," March 6, 2000.

DoD IG Instructions:

IGDINST 5015.2, "Records Management Program," November 7, 2007.

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.

DefenseReady is designed to organize, manage, and track personnel, billets, training, security clearance data, and make it available in a web interface to DoD OIG managers and employees without having to access multiple authoritative systems from which the data is synchronized. Data is synchronized and/or manually entered from the Defense Civilian Personnel Data System (DCPDS) and Forth Estate Manpower Tracking System (FMTS). The records contain: Name, Social Security Number (SSN), Other ID Number (DoD Employee ID / EDIPI), Citizenship, Legal Status, Gender, Race/Ethnicity, Birth Date, Place of Birth, Personal Cell Telephone Number, Home Telephone Number, Personal Email Address, Mailing/Home Address, Security Clearance, Disability Information, Employment Information, Military Records, Emergency Contact, Education Information

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

Physical Access Risks - Entry to the equipment necessary to obtain information is restricted by the use of Security Guards, Cipher Locks, Identification Badges, Key Cards, and Closed Circuit TV (CCTV). Computer systems, records and magnetic tapes are maintained in limited access controlled and monitored areas.

System Access Risks - Computers are controlled with Common Access Cards (CAC), and computer screens automatically lock after a preset period of inactivity with CAC required for re-entry. Access to any DoD OIG computers is restricted to authorized users only.

Personnel Risks - All individuals accessing this system of records are required to have completed Information Assurance and Privacy Act Training.

Overall Risks - Security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.

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.

☐ **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.

(2) If "No," state the reason why individuals cannot object.

The information is compiled from information collections that already exist. The information is gathered from information that the individual has already provided.

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.

The information is compiled from information collections that already exist. The information is gathered from information that the individual has already provided.

--

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.

The information is compiled from information collections that already exist. The information is gathered from information that the individual has already provided. Privacy notifications apply to the separate information collections, prior to the compilation in the EBAS system.

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.