



PRIVACY IMPACT ASSESSMENT (PIA)

For the

The North Central Region Productivity (NCRP) Toolkit
--

North Central Regional Director's Office
--

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.

5 U.S.C. 301, Departmental Regulations;
10 U.S.C. 3013, Secretary of the Army;
Army Regulation 690-200, General Personnel Provisions; and E.O. 9397 (SSN).

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 North Central Region Productivity (NCRP) Toolkit is a collection of tools utilized by the North Central Region of the Civilian Human Resources Agency (CHRA) to access reports, perform audits, manage access control, work with foreign entitlements, and perform staffing duties for the Medical Command (MEDCOM) utilizing the Aladdin staffing suite. The type of personal information collected on individuals is contained in a resume or employee's application. The type of PII collected is personal, employment, and military information. The following are the tools in NCRP:

1. Aladdin Suite: The Announcement and Application Log and Rating suite (Aladdin) recruitment tool used by the MEDCELL Team and Medical Command (MEDCOM) for hiring medical personnel.
2. NCCPC Intranet: Used for general reporting and information sharing.
3. Internal Audit: Provides functionality for internal auditing, quality control, and for checking regulatory and procedural compliance for personnel actions.
4. Processing Audit: Used by the processing centers at all CHRA regions to capture issues with personnel actions which do not conform to the Guide to Processing Personnel Actions (GPPA) 5 Code of Federal Regulations (5 CFR).
5. SARS: The System Access Request System (SARS) is used to grant and track access to Defense Civilian Personnel Data System (DCPDS), Customer Service Unit (CSU), and Business Objects XI (BOXI).
6. SAFE: The Support and Assistance for Foreign Entitlements (SAFE) tool is used to track eligibility for foreign entitlements.
7. SRC: Special Retirement Coverage and Audit tool (SRC) was originally developed to enable a Civilian Personnel Evaluation Agency (CPEA) audit of Special Retirement Coverage (SRC) employees, this tool is used to track data validity and potential policy/regulation violations in employee data.

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

Internal and external risks are associated with the protection of PII; however, risks are minimized to an acceptable level. Safeguards, such as network firewalls, software and hardware based intrusion detection, encryption, reverse web proxy (in the case of Aladdin/MEDCELL), and best business practices for web development and database management are employed to detect and minimize unauthorized disclosure, modification, and/or destruction of data; thus we believe the risk to the individual's privacy to be minimal.

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.

The majority of NCRP Toolkit interfaces with DCPDS personnel data that exists for all Army Civilian Employees or other data input by management. However, in the case of Aladdin, applicants must submit resumes and PII to be considered for federal employment.

(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.

The majority of the NCRP Toolkit interface with DCPDS personnel data that exists for all Army Civilian Employees or other data input by management. However, in the case of Aladdin, applicants consent to the specific use of PII by submission of resumes.

(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.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

The Aladdin/MEDCELL suite does include tools that gather PII directly from the public in the form of applicants' resumes and other application based data required when applying for employment with the federal government. This system provides a Privacy Act Statement for applicants to review.

The other NCRP Toolkit do not interface directly with end users as the hosted tools are productivity or quality control based audits intended for personnelists. These are internal tools used only for staffing personnel and do not provide any privacy warning.

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.