



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Public Health Survey Builder Software (Verint® Enterprise Feedback Management)

US Army Medical Command - DHP Funded Web Site

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.

10 U.S.C. 3013, Secretary of the Army; 5 U.S.C. 7902, Safety Programs; 29 U.S.C. 668, Programs of Federal Agencies; 29 CFR 1910, Occupational Safety and Health Standards; Army Regulation 40-5, Preventive Medicine; E.O. 12223, Occupational Safety Health Programs for Federal Employees; 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 Public Health Survey software, Verint Enterprise Feedback Management, is a commercial web-based product used by the US Army Public Health Command (USAPHC) to build and deploy surveys and questionnaires to support the public health mission. Data are used to identify needs and assess experiences with programs, view statistical reports, and export responses to databases. Questionnaires are also being developed to support the monitoring of the incidence and trends of diseases, injuries, behavioral health conditions, and other health-related outcomes. Other surveys covered in this PIA include: conference workshops, training experiences, customer service/satisfaction and overall support to the mission of the USAPHC as the Army's public health authority.

Categories of individuals collected by the system can include Army active duty, National Guard, Reserve, Army retired, government civilian employees and military family members.

The types of personal information collected can include: Name, Social Security Number, Birth Date, Race, Ethnicity/Gender, Medical Information and Work Contact information (Phone and Email). Per DODI 1000.30, Reduction of SSN Use within DoD, USAPHC only uses the SSN for database (computer) matching. Without a common identifier agreed to and implemented by all of the information systems from which USAPHC received data, such as the SSN, the USAPHC does not have a method to inter-relate data received from each of the respective systems.

This PIA updates the PIA approved on 2 April 2012.

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

The privacy risks associated with the PII/PHI collected are unauthorized access and unauthorized disclosure of PII. Security safeguards are in place to mitigate these risks. These security measures are outlined in Section 3 below.

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.

The PII will be shared with USAPHC personnel who have a need-to-know this information.

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.

An individual can object to the collection by not supplying the information. In accordance with the Privacy Act Statement associated with this system, furnishing PII is voluntary, but failure to provide this information will result in inaccurate information in the system and inaccurate reports.

(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.

An individual can object to the specific uses of their PII by not supplying the information. The specific uses of their PII is provided in the Privacy Act Statement associate with this application. The specific uses of their PII are addressed in the Privacy Act Statement associated with this system. Failure to provide this information will result in inaccurate information in the system and inaccurate reports.

(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.

Privacy Act Statement is delivered via a splash screen on the web site.

AUTHORITY: 10 U.S.C. 3013, Secretary of the Army; 5 U.S.C. 7902, Safety Programs; 29 U.S.C. 668, Programs of Federal Agencies; 29 CFR 1910, Occupational Safety and Health Standards; Army Regulation 40-5, Preventive Medicine; E.O. 12223, Occupational Safety Health Programs for Federal Employees; and E.O. 9397 (SSN).

PRINCIPAL PURPOSE(S): Primary uses are to: Aid in preventive health and communicable disease control programs; compile statistical data; conduct research; determine suitability of persons for service or assignments; evaluate customer service/satisfaction; determine professional certification.

ROUTINE USE(S): Information will be used only within the assigned activity and will not be released to any other staff activity.

DISCLOSURE: Information is voluntary, however, failure to provide all requested information will result in inaccurate information in the system and inaccurate reports.

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.