



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Occupational and Environmental Health Readiness System - Industrial Hygiene (DOEHRS-IH)

Defense Health Agency (DHA)

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

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. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 55, Medical and Dental Care; 29 U.S.C. 651, Congressional Statement of Findings and Declaration of Purpose and Policy; DoDD 4715.1E, Environment, Safety, and Occupational Health (ESOH); DoDI 6055.1, DoD Safety and Occupational Health (SOH) Program; DoDI 6055.05, Occupational and Environmental Health (OEH); DoDI 6055.17, DoD Installation Emergency Management (IEM) Program; DoDI 6200.03, Public Health Emergency Management Within the Department of Defense; and E.O. 9397 (SSN), as amended.

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 purpose of the DOEHRS-IH system is to establish a database for longitudinal exposure recordkeeping and reporting to support occupational and environmental health surveillance (OEHS), public health surveillance, health risk management, and medical surveillance; and to provide this data in support of medical treatment, occupational and environmental illness evaluations, disability determinations, and claims adjudication. Another purpose of this system is to complete the collection and analysis of threat exposures for designated event areas in all phases of military operations and as a result of actual or perceived natural disasters, hazardous material releases, chemical/biological/nuclear accidents which may affect DoD-affiliated personnel. DOEHRS-IH is fully deployed to the Army, Navy and Air Force.

Individuals covered by the DOEHRS-IH system include:

Members of the Armed Forces; Department of Defense (DoD)-affiliated personnel (includes DoD civilian employees, DoD contractors, and DoD foreign national employees) who live or work in areas requiring longitudinal data related to occupational, environmental, or public health. Spouses and dependents of members of the Armed Forces and DoD-affiliated personnel if such spouse or dependent is in the area of a perceived or actual occupational, environmental, or public health event.

The types of personal information about individuals collected in the system individuals include:

Personal descriptors, ID numbers, event based information, demographics, and life information.

DOEHRS-IH is owned by Defense Health Agency (DHA) and managed under the Defense Health Services Systems (DHSS) Program Office.

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

The privacy risk posed by the collection, use, and sharing of information is that a user may inadvertently disclose personally identifiable information (PII) to an unauthorized user. This risk has been minimized through system design and implementation of various administrative, technical, and physical security controls.

DHSS government employees and contractors follow DHSS and other government policies provided in annual Health Insurance Portability and Accountability Act (HIPAA) and Privacy Act Training. Tier III vendors have internal company policies which they follow in the case of security breaches. All personnel accessing the Out-of-Band VPN (and any DISA servers) read, sign, and adhere to policies in the JMIS Secure Remote Computing Rules of Behavior.

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.

Ultimately, DOEHRS-IH will be interfaced with iEHR. DOEHRS-IH includes corporate reporting, which will provide timely and efficient worldwide access of data and information to users throughout the Department of Defense (DoD), including Military Treatment Facility (MTF) Commanders, Industrial Site Commanders, Deployed Site and MTF Commanders, Lead Agents, and Installation Agencies. However, only personnel with the appropriate level of access will be able to see PII, and they will only have access to data specific

to their area of responsibility.

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.

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.

DOEHRS-IH is required to support administration of Federal Worker's Compensation. The Federal Worker's Compensation Program continues to track individuals through the use of the Social Security Number (SSN). When Federal Worker's Compensation claims are filed, DOEHRs-IH is required to provide relevant exposure records. To ensure accurate records are released, the SSN is utilized in addition to other direct identifiers such as name and address. OSHA Standard Number 1910.1020 requires employers to provide "employees and their designated representatives a right of access to relevant exposure and medical records". OSHA requires records be kept for period of employment plus thirty (30) years. To ensure accurate exposure records are released, the SSN is utilized in addition to other direct identifiers such as name and address.

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.

This statement serves to inform you of the purposes for collecting your personal information into the Defense Occupational and Environmental Health Readiness System – Industrial Hygiene (DOEHRS-IH) and how it will be used.

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 29 U.S.C. 651, Congressional Statement of Findings and Declaration of Purpose and Policy; DoDI 6055.1, DoD Safety and Occupational Health (SOH) Program; DoDI 6055.05, Occupational and Environmental Health (OEH); and E.O. 9397 (SSN), as amended.

PURPOSE: To collect your data regarding exposure to occupational health hazards for recordkeeping, health surveillance, treatment, and other purposes.

ROUTINE USES: Your records may be disclosed to support medical care, research, and to other federal agencies for determination and adjudication of pending claims. Use and disclosure of your records outside of DoD may also occur in accordance with the DoD Blanket Routine Uses published at <http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx> and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a(b)).

DISCLOSURE: Although providing information is voluntary, in that you will not be subject to any criminal penalties, failure to provide this information may result in you being removed from your duties, punished by your commander or supervisor, and/or subject to other negative actions.

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.