



PRIVACY IMPACT ASSESSMENT (PIA)

For the

| |
|---|
| Inquiry and Case Management System (ICMS) |
|---|

| |
|---|
| Defense Human Resources Activity (DHRA) |
|---|

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.

38 U.S.C. 43, Employment and Reemployment Rights of Members of the Uniformed Services; 5 U.S. C. 574, Confidentiality; 5 U.S.C. Part I, Chapter 5, Subchapter IV, Alternative Means of Dispute Resolution in Administrative Process; 42 U.S.C. 300hh-11 (d)(3), National Disaster Medical System; 20 CFR 1002, Regulations Under the Uniformed Services Employment and Reemployment Rights Act of 1994; 5 CFR 353, Restoration to Duty from Uniformed Service or Compensable Injury; DoD Directive 1250.01, National Committee for Employer Support of the Guard and Reserve (NCESGR); DoD Instruction 1205.22, Employer Support of the Guard and Reserve; and DoD Instruction 1205.12, Civilian Employment and Reemployment Rights of Applicants for, and Service Members and Former Service Members of the Uniformed Services.

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.

To record information related to the mediation of disputes and answering of inquiries related to the USERRA; by tracking case assignments and mediation results of potential conflicts between employers and the National Guard, Reserves, or National Disaster Medical System (NDMS) members they employ; and by reporting statistics related to the Ombudsman Program in aggregate and at the state committee-level. These records are also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness and conducting research.

ICMS maintains the following categories: Individual's full name, home address, phone number, email address; affiliated Service, assigned military unit, and rank; ESGR case number; type of Uniformed Services Employment and Reemployment Rights Act (USERRA) issue; employer's representative name, company name, employer type, work phone, email and address; name, username, email and state committee/ESGR affiliation of ESGR employee, contractor, or volunteer that handles an inquiry or mediation case; case notes; state where case occurred.

(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 collected are information mishandling and improper release to personnel with other than need to know. To safeguard such information, access to ICMS and the PII it holds is maintained in a secure, password protected electronic system that utilizes security hardware and software. Additional safeguards are provided via the use of user names and passwords with 2-factor authentication, intrusion detection system, encryption, Common Access Cards, firewalls, virtual private networks, DoD Public Key Infrastructure Certificates, and role-based access controls. System databases are also stored in controlled rooms secured via combination locks, cipher locks, key cards, identification badges, closed circuit televisions, and security guards. Backups containing sensitive data are encrypted and all backups are secured off-site.

Access to records is limited to those who require the records to perform their official duties, consistent with the purpose for which the information was collected. All personnel whose official duties require access to the information are trained in the proper safeguarding and use of the information via the completion of initial and refresher privacy training. Periodic security audits and regular monitoring of users' security practices are also conducted, while visitors are monitored via the use of visitor registers.

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.

To the Department of Labor for Congressionally-mandated USERRA reporting (38 U.S.C. Employment and Reemployment Rights of Members of the Uniformed Services, section 4432, Reports).

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.

Individuals may object to the collection of their PII by not providing their information to ESGR; however, failure to provide accurate contact information and other solicited information may delay or prevent ESGR from processing the request.

(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.

SGR cannot respond to inquiries or provide mediation support without the collection of the requested PII.

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 checked="" type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

USERRA Inquiry Form:
 Authority: 38 U.S.C. 43, Employment and Reemployment Rights of Members of the Uniformed Services; 5 U.S.C. 574, Confidentiality; 5 U.S.C. Part I, Chapter 5, Subchapter IV, Alternative Means of Dispute Resolution in Administrative Process; 42 U.S.C. 300hh-11(d)(3), National Disaster Medical System; 20 CFR 1002, Regulations Under the Uniformed Services Employment and Reemployment Rights Act of 1994; 5 CFR 353, Restoration to Duty from Uniformed Service or Compensable Injury; DoD Directive 1250.01, National Committee for Employer Support of the Guard and Reserve (NCESGR); DoD Instruction 1205.22, Employer Support of the Guard and Reserve; and DoD Instruction 1205.12, Civilian Employment and Reemployment Rights of Applicants for, and Service Members and Former Service Members of the Uniformed Services.

Purpose: To support the ESGR Ombudsman Program by tracking assistance provided to members of the Uniformed Services, to include the National Disaster Medical System; by recording information related to answering inquiries related to the USERRA; and by reporting statistics related to the Ombudsman Program in aggregate and at State committee-level. The applicable Privacy Act System of Records Notice is DHRA 16, Inquiry and Case Management System found at <http://dpcl.d.defense.gov>

Routine Use(s): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.

To the Department of Labor for Congressionally-mandated USERRA reporting (38 U.S.C. Employment and Reemployment Rights of Members of the Uniformed Services, section 4432, Reports).

Applicable Blanket Routine Use(s) are: (1) Law Enforcement Routine Use, (2) Disclosure When Requesting Information Routine Use, (3) Disclosure of Requested Information Routine Use, (4) Congressional Inquiries, (8) Disclosure to the Office Personnel Management Routine Use, (9) Disclosure to the Department of Justice for Litigation Routine Use, (12) Disclosure of Information to the National Archives and Records Administration Routine Use, (13) Disclosure to the Merit systems Protection Board Routine Use, and (15) Data Breach Remediation Purposes Routine Use.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: <http://dpcl.d.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx>.

Disclosure: Voluntary; however, failure to provide accurate contact information and other solicited information may delay or prevent ESGR from processing the request.

USERRA Support Request:
 Authority: 38 U.S.C. 43, Employment and Reemployment Rights of Members of the Uniformed

Services; 5 U.S.C. 574, Confidentiality; 5 U.S.C. Part I, Chapter 5, Subchapter IV, Alternative Means of Dispute Resolution in Administrative Process; 42 U.S.C. 300hh-11(d)(3), National Disaster Medical System; 20 CFR 1002, Regulations Under the Uniformed Services Employment and Reemployment Rights Act of 1994; 5 CFR 353, Restoration to Duty from Uniformed Service or Compensable Injury; DoD Directive 1250.01, National Committee for Employer Support of the Guard and Reserve (NCESGR); DoD Instruction 1205.22, Employer Support of the Guard and Reserve; and DoD Instruction 1205.12, Civilian Employment and Reemployment Rights of Applicants for, and Service Members and Former Service Members of the Uniformed Services.

Purpose: To support the ESGR Ombudsman Program by tracking assistance provided to members of the Uniformed Services, to include the National Disaster Medical System; by recording information related to the mediation of disputes and answering of inquiries related to the USERRA; by tracking case assignments and mediation results of potential conflicts between employers and the Service members they employ; and by reporting statistics related to the Ombudsman Program in aggregate and at State committee-level. The applicable Privacy Act System of Records Notice is DHRA 16, Inquiry and Case Management System found at <http://dpcl.d.defense.gov>.

Routine Use(s): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.

To the Department of Labor for Congressionally-mandated USERRA reporting (38 U.S.C. Employment and Reemployment Rights of Members of the Uniformed Services, section 4432, Reports).

Applicable Blanket Routine Use(s) are: (1) Law Enforcement Routine Use, (2) Disclosure When Requesting Information Routine Use, (3) Disclosure of Requested Information Routine Use, (4) Congressional Inquiries, (8) Disclosure to the Office Personnel Management Routine Use, (9) Disclosure to the Department of Justice for Litigation Routine Use, (12) Disclosure of Information to the National Archives and Records Administration Routine Use, (13) Disclosure to the Merit systems Protection Board Routine Use, and (15) Data Breach Remediation Purposes Routine Use.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: <http://dpcl.d.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx>.

Disclosure: Voluntary; however, failure to provide accurate contact information and other solicited information may delay or prevent ESGR from processing the request.

For phone calls, each Individual is asked to consent to the specific use of their PII. The following text must be read to the individual before providing their PII on the phone:

"Before you provide us any personal information. I need to advise you of how ESGR Ombudsman Services will use the information that you provide to us. Communications with ESGR Ombudsmen are governed by Federal Statute, which generally provides confidentiality on related communications. The information you provide will be relayed to an Ombudsman, who will contact you to gain additional details and also speak with your employer to assist in reaching a resolution. If you DO NOT wish anything you say be communicated to the Ombudsman assigned to help resolve your issue, please tell me now. Having been advised; do you wish to proceed with the opening of a case, with ESGR?"

Following the phone call, ESGR provides the Privacy Act Statement to the caller via an auto-generated email.

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.