



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Employer Support of the Guard and Reserve Public Website (www.esgr.mil)
-------------------------------------------------------------------------

Employer Support of the Guard and Reserve (ESGR)
--------------------------------------------------

### **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. 1588, Authority to Accept Certain Voluntary Services; DoD Instruction 1205.22, Employer Support of the Guard and Reserve; DoD Instruction 8550.01, DoD Internet Services and Internet-Based Capabilities; DoD Instruction 8500.01 Cybersecurity.

**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 system is to support the Employer Support of the Guard and Reserve (ESGR) mission to: facilitate and promote a cooperative culture of employer support for National Guard and Reserve service by developing and advocating mutually beneficial initiatives; recognize outstanding employer support; increase awareness of applicable laws and policies; resolve potential conflicts between employers and their service members; and act as the employers' principal advocate within DoD. The PII contained in this system is used to create user accounts for a small subset of ESGR volunteers who handle public affairs, so that they are able to login to the website to contribute content (e.g., news and upcoming events) to the site.

The types of personal information stored in ESGR.mil include: volunteer member's full name, email address, and state.

(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 information access, personal information is maintained in a secure, password protected electronic system that utilizes security hardware and software to include: encryption, firewalls, intruder detection, virtual private network, and role-based access controls. Physical controls include security guards, identification badges, key cards, cipher locks, combination locks, and closed circuit TV. Access to records is limited to those officials, i.e. website administrators, 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.

**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.

Individuals may object to the collection of their PII by not providing their information to ESGR; however, failure to provide the requested information may impede, delay, or prevent further processing of user accounts.

(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.

ESGR cannot create a State User account to log into the system without the collection of the requested information.

(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.

**Privacy Act Statement**

**Privacy Advisory**

**Other**

**None**

Describe each applicable format.

DD Form 2875 System Authorization Access Request (SAAR)
Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
Principal Purpose: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
Routine Uses: None.
Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

**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.**