# PRIVACY IMPACT ASSESSMENT (PIA)

## For the

| |
|---|
| Family and Employer Programs and Policy (FEPP)<br>Communications ListServ (GovDelivery) |
| Family and Employer Programs and Policy (FEPP) |

## 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 USC § 4333, Outreach; DoDD 1250.01, National Committee for Employer Support of the Guard and Reserve; DoD 1205.22, DoDI 1205.12, Employer Support of the Guard and Reserve; Civilian Employment and Reemployment Rights for Service Members, Former Service Members and Applicants of the Uniformed Services; DoDI 1205.22, Employer Support of the Guard and Reserve; DoDI 1342.28, DoD Yellow Ribbon Reintegration Program.

**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.

FEPP collects e-mail addresses to support the outreach and marketing campaigns for Employer Support of the Guard and Reserve (ESGR) and Yellow Ribbon Reintegration Program (YRRP). Emails are provided by individuals interested in receiving program information. DMDC provides FEPP emails for new accessions and recently promoted members of the Guard and Reserve to support emailing this audience information about ESGR and YRRP.

Per DoDI 1205.12 and DoDI 1205.22, ESGR is required to increase awareness of applicable Uniformed Services Employment and Reemployment Rights Act related laws and policies.

DoDI 1342.28 requires providing information, services, referrals, and proactive outreach throughout the deployment cycle to mitigate the challenges of transitions between duty statuses, family separation, and reintegration into families, careers, and communities.

A variety of communication platforms, including social media, blogs, websites, e-mail marketing, and traditional media outlets are used to reach stakeholders.

(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, personal information is maintained in a secure, password protected electronic system that utilizes security hardware and software. Physical controls include security guards, identification badges, key cards, multi-factor authentication, retinal, fingerprint scans, and closed circuit TV. Technical controls include the use of user identification, password, intrusion detection system, encryption, Common Access Card, biometrics, firewalls, and virtual private network. Administrative controls include periodic security audits, regular monitoring of users' security practices, methods to ensure only authorized personnel access to PII, encryption of backups containing sensitive data, backups secured off site, and the use of OMB MAX Integration.
- Individuals are given the opportunity to opt-out of the system. GovDelivery has implemented security policies and procedures in accordance with NIST guidelines.

**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.

Personnel subscriptions are supplied by the individual voluntarily to receive updates via https:// guardreserves.com. Individuals are provided with instructions to opt-out of the ListServ at any time through multiple methods. Currently, any user that comes to the web site can opt-in to receive updates by providing an e-mail address. At any time, that user can unsubscribe from GovDelivery and their record will be permanently deleted.

(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.

For accessions and promotions, Guard and Reserve members are not given the ability to opt-out of email being sent to DoD email provided by DMDC.

**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. | There is no PII data collected outside of e-mail addresses. Individuals can review the Privacy Policy by clicking on a link on the subscription page. Each page of the GovDelivery website has a link to the Privacy Policy. Users can create a password to enter their prescription preferences. |

**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.**