



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

BUPERS Online (BOL)

Department of the Navy - BUPERS

### 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.

SORN NM05000-2 authorities:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN), as amended.

Other authorities:

BUPERS Instruction 5239.1B, Bureau of Naval Personnel (BUPERS) Information Systems Security (INFOSEC) Program, April 5, 2001

CJCSI 6510.01, Chairman of the Joint Chiefs of Staff Instruction, Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND), March 18, 2005

DoDI 8510.01, Department of Defense, Information Assurance Certification and Accreditation Process (DIACAP) Instruction, 28 NOV 2007

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014.

DoN IA Publication 5239-13 Volume II, Site, Installed Program of Record, and Locally Acquired Systems,

**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.

BUPERS On Line (BOL) is an applications hosting framework that provides a Single Sign On (SSO) authentication for various MPT&E applications hosted in the Millington Data Center. Credential verification is completed via CAC/PKI verification using the DEERs authentication of the members Department of Defense Intelligence Digest (DODID), as well as, certificate verification via DISA's Certificate Revocation Listing (CRL). Once credentials have been verified BOL then allows access to the various applications based on the member's role/access level. If a user requests additional accesses outside of the normal business rules, the "need to know" is verified using the System Authorization Access Request Navy (SAAR-N) process.

Sailors are granted (as a default) access to BOL and the data required for authentication is derived from the ITEMPO db. Civilians and contractors provide their PII via the SAAR-N process to establish their BOL account. Administrators input this information for individual account establishment.

BOL is operated by PERS-54 within the Navy Personnel Command (NPC). BOL supports NPC activities with local users, users located at the Navy Annex in Washington, DC, Active Duty and Reserve service members and other authorized users of applications hosted within BOL. Users access the system using a web browser over the Internet. Users are only required to have Internet access, a web browser and appropriate authorization credentials.

The BOL System is a highly-available, fault tolerant system with load balancing or redundancy built into the system wherever feasible. The system is designed for delivery of content and applications through the web browser. Applications are supported in a three-tier logical design, physically implemented over two or three tiers. Database servers are set up in active-active clusters. Web servers deliver the user interface and application logic tier in most cases. The web servers are hardware load balanced. The BOL program provides portal/front end services to authenticate, via common access card (CAC), authorized users for access to one or more of the various systems/programs/applications resident on BOL system/infrastructure.

Personal information collected: Name, SSN, DoD ID Number, Birth Date.

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

Individual user's password is compromised. This risk is primarily the responsibility of the system user to safeguard. Since PII data is flushed from the cache the only identified vulnerability is with the user. BOL user passwords conform to current DoD requirements. Primary users are typically Navy based and have CAC access.

**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.

PII information is not mandatory. However, there is no mechanism in place to validate user access in the absence of PII data. An individual may refuse/decline to establish an account/login.

(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.

Establishment of user account provides 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.

A PAS is provided on the SAAR-N form for BOL account establishment for civilians and contractors.

**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.**