PRIVACY IMPACT ASSESSMENT (PIA)

For the

FLAG MANAGEMENT AND DISTRIBUTION SYSTEM (FMDS)
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**	☒	**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	DADMS ID: 87167
☐	**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 N01070-5, NM05000-2 and N01070-16.

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 N01070-5 Authorites:

10 U.S.C. 5013, Secretary of the Navy

SORN N01070-16 Authorities:

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 5013, Secretary of the Navy
E.O. 9397 (SSN), as amended

SORN NM05000-2 Authorities:

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

A Chief of Naval Personnel letter to Navy Flag Officer Management Office dated 22 April 2014 and in conjunction for the Chief of Personnel, PERS-00F Charter dated 2 January 2014, the collection of PII data is required in order to manage the education, training, detailing, promotion, retirement and the overall management decisions pertaining to Active and Reserve flag officers. This database will also

collect/maintain PII data on retired flag officers per direction issued by the Chief of Naval Operations.

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.

This functionality has existed for many years but it was previously done by manually collecting and aggregating the data in order to provide the reports required by the CNO.

The Flag Management and Distribution System (FMDS) is used by OPNAV N00F to meet the requirements set forth in OPNAV 1520.43: the development and distribution of Navy Flag officers. The functionality of FMDS allows OPNAV N00F to provide the Chief of Naval Operations (CNO) and Deputy Chief of Naval Operations (Manpower, Personnel, Training, and Education) (CNO (N1)) the information required for flag officer development, tracking of individual progression, administrative coordination, financial oversight, and flag officer assignments. Further, through report generation and metric analysis, FMDS allows N00F to meet the spontaneous and periodic reporting requirements of the CNO and CNO N1. FMDS contains the professional data of a flag officer, e.g., billet and command history, formal education, Navy training, qualifications. FMDS allows OPNAV N00F to provide the Chief of Naval Operations (CNO) and Deputy Chief of Naval Operations (Manpower, Personel, Training, and Education) (CNO (N1)) the information required for flag officer development, tracking of individual progression, administrative coordination, financial oversight, and flag officer assignments. It will also be used to maintain a directory of retired Navy flag officers for the purpose of providing briefings and outreach materials, and facilitating interaction between retired and active duty Navy flag officers.

FMDS is hosted in the BUPERS ONLINE (BOL) environment.

Personal information collected includes: Name, SSN, citizenship, gender, race/ethnicity, birth date, personal cell telephone, home telephone number, personal email address, mailing/home address, religious preference, security clearance, marital status, Military Records: Additional Qualification Designator (AQD), Navy Officer Billet Classification (NOBC); Education information: Military courses completed and all military training; Employment information: Post-retirement flag officer employment history; and Spouse Information: Name and any nicknames.

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

The collection of personal information presents a risk because of the potentially sensitive nature of the information and the consequence of the data being mishandled, which could lead to unwarranted invasion of the individual's privacy. This risk is mitigated by ensuring that access to the data is strictly controlled and by making sure that all administrative, technical, and physical controls are in place to protect the data.

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. Secretary of the Navy (SECNAV), Chief of Naval Operations (CNO), and Vice Chief of Naval Operations (VCNO)

☐ **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. Lockheed Martin and SAIC support BOL in PERS-54. These contractors have signed letters of non-disclosure and are fully aware of their responsibility for protecting PII.

☐ **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.

Each member is provided with a Privacy Act Statement (PAS) when they are announced as a new flag officer select. The flag officer has the option to allow or disallow us to collect and distribute all or some of the data that we put in our reports.

(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.

Each member is provided with a Privacy Act Statement (PAS) when they are announced as a new flag officer select. The flag officer has the option to allow or disallow us to collect and distribute all or some of the data that we put in our reports.

(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.

Each member is provided with a Privacy Act Statement (PAS) when they are announced as a new flag officer select. The flag officer has the option to allow or disallow us to collect and distribute all or some of the data that we put in our reports.

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.