PRIVACY IMPACT ASSESSMENT (PIA)

For the

Business Information System (BIS)
Department of the Navy - COMPACFLT - Pacific Missile Range Facility

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	DITPR ID: 1598 DITPR DON ID: 20467
☐	**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 UII: 007-000006837

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 NM07421-1

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 authorities:

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
E.O. 9397 (SSN), as amended.

Other authorities:

5 U.S.C. Chapters 53, 55, 61 and 63, Pay Rates and Systems, Pay Administration, Hours of Work, and Leave
31 U.S.C. Chapter 35, Accounting and Collection
DoD Financial Management Regulation (DoDFMR) 7000.14-R, Vol. 8, Chapter 5
COMUSFLTFORCOM/COMPACFLTINST 3624.1B

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.

PMRF has a large reimbursable customer base and each sponsor has a unique set of reporting and cost tracking requirements. Each customer must be charged for direct costs, which are fair, competitive, and justifiable. Sponsors routinely request a detailed explanation of every dollar charged to their accounts by operation number and field support unit, even down to the name of the asset. These detailed reports are not available in the Standard Accounting and Reporting System (STARS/fl) (the standard DFAS accounting system). The majority of charges incurred by most of these customers are for contractor support. The charging routines are very complex and generate thousands of transactions. In an attempt to better track costs and provide detailed operations data, PMRF designed and developed the Oracle based BIS which contains and maintains this specific kind of data.

From DITPR DON: The Business Information System (BIS) is used to provide cost data for the United Range Reporting List (URRL) per Navy instruction COMUSFLTFORCOM/COMPACFLTINST 3624.1B from the U.S. Fleet Forces Command N73 (coordinator of all fleet training range requirements with the Navy Range Office (NRO) , OPNAV N433). Additionally, BIS is the source of data for the Uniform Financial Management System for the DOD MRTFB. BIS is an automated tool (web-based) used to support the PMRF's program management process which includes planning, estimating, budgeting, timecards, credit cards, travel and contractor cost tracking. Information is entered once and validated at its source. Automatic date and funding level checks are built into the system. Rolling up operational data and transferring it electronically to STARS/FL have eliminated a significant amount of manual data input into STARS/FL. In addition, all PMRF costs are entered with associated function support unit (FSU). FSU cost tracking allows range personnel to track the costs of supporting and maintaining specific items, down to the radar. This level of granularity is required to populate the major range test facility and base (MRTFB) exhibits and budgets.

Personal information collected includes: Name, SSN, Birth Date, citizenship, Personal Cell Telephone Number, Home Telephone Number, Mailing/Home Address, Security Clearance, Financial Information:bank name, account number, routing number; Employment Information: work history and resume; Emergency Contact, and Education Information: level of education and degree.

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

The data collected and stored on BIS is always at risk of unauthorized access due to number of users with access. The known threats are disgruntled employees, social engineering, and natural causes (i.e. fire, storms, etc.). Due to these possibilities, there are proper security and access controls in place to secure the PII data. All authorized users access approved BIS information via NMCI network. Each user is PKI enforced and limited to access BIS information based on their roles and responsibilities. Administrators and organizational managers determine users needs which are then processed by the BIS administrators only. BIS administrators review logs on a weekly basis.

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. PMRF Finance, PMRF Range Contract Support

☐ **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.

(2) If "No," state the reason why individuals cannot object.

Civilian employees provide their personal information as part of the hiring process. PCS orders contain the military member's personal information. The required information from these two sources ins entered into BIS by a system administrator.

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.

Civilian employees provide their personal information as part of the hiring process. PCS orders contain the military member's personal information. The required information from these two sources ins entered into BIS by a system administrator.

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.

Civilian employees provide their personal information as part of the hiring process. At this time they are presented with and sign a privacy act statement.

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.