PRIVACY IMPACT ASSESSMENT (PIA)

For the

Integrated Management/Processing System (IMPS)
Department of the Navy - Naval Research Laboratory (NRL)

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: 45 DITPR DON ID: 14965
- ☐ **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: 007-000006557

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 NM05000-2; OPM/GOVT-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:

NM05000-2: Program Management and Locator System
10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5014, Headquarter, Marine Corps
E.O. 9397 (SSN), as amended

OPM/GOVT-1: General Personnel Records.

5 U.S.C. 1302 Regulations
5 U.S.C. 2951 Reports to the Office of Personnel Management
5 U.S.C. 3301 Civil service; generally
5 U.S.C. 3372 General provisions
5 U.S.C. 4118 Regulations
5 U.S.C. 8347 Administration; regulations
E.O. 9397 (SSN), as amended
E.O. 9830 Amending the Civil Service Rules and providing for Federal personnel administration
E.O. 12107 Relating to the Civil Service Commission and labor-management in the Federal Service

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.

Integrated Management Processing System (IMPS) is an integrated network of systems and software that together make up the official business system(and the financial system of record) for the Naval Research Laboratory(NRL). It is a comprehensive information system whose mission is to provide both transactional processing and advanced management information query capabilities to NRL. The personal information included in IMPS is that which is required to process labor, travel and personal payment financial transactions, locate and contact NRL personnel (both under routine and emergency situations); notify next of kin when necessary; process employment applications, security investigations and clearance requests, and manage/report on the NRL workforce.

Personal information includes: Name, social security number, citizenship, gender, race/ethnicity, birth date, place of birth, personal cell telephone number, home telephone number, personal email address, mailing/ home address, security clearance, financial information, medical information, disability information, employment information, emergency contact, and education information.

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

There are threats from computer hackers, disgruntled or careless employees, state sponsored information warfare and acts of nature (such as fire, flood, etc.). Because of this possibility, appropriate security, backup and access controls listed in this PIA are in place and working effectively. IMPS managers are vigilant in reviewing access requests to make sure the request appears to be legitimate for the person's job and is authorized by appropriate division management or Admin Office. Backups are monitored closely, are encrypted and are duplicated off-site. All IMPS users have gone through extensive background and employment investigations and annual Security, PII and Information Assurance training. All IMPS screens and reports containing sensitive PII have the appropriate warning banner on their top line(s). NRL has strict security measures (e.g. guarded gates, NRL badging and investigation requirements) and the IMPS computer rooms (primary and backup locations) are secured with environmental alarms and cipher locks. Access to these locations is also limited to individuals who have a need to work in that area and vendor maintenance personnel are always supervised. NRL maintains an aggressive network monitoring program and IMPS is kept compliant with the DoD Information Assurance Vulnerability Management Program (IAVM). IMPS servers reside behind the MISNet router (which functions as a firewall).

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. Personnel working in NRL Human Resources, Security and Finance areas will have access to forms and records for processing.

☒ **Other DoD Components.**

Specify. Defense Finance and Accounting Service (DFAS)

☐ **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.

Personal information is collected from the DON Civilian Authoritative Data Source (DONCADS), the Defense Civilian Payroll System (DCPS) and the Defense Travel System (DTS) so the individual does not have the opportunity to object to the collection.

Other data is provided by the individual during the recruiting/hiring process, when completing Travel or Miscellaneous Reimbursement claims and Security Investigation/Badge request forms. Information is provided as a condition of employment or must be provided to process claims.

Information required on Locator/Emergency Notification forms is voluntary. Failure to provide this information however would make it difficult or impossible to locate or notify the employee or their emergency contacts.

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.

Information collected from the above systems or from the individual are used as a condition of

employment, to process claims, or for contacting family members or designated individuals in the case of an emergency.

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 Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), is provided on all forms that collect PII data for this system, allowing the individual to make an informed decision about providing the information. The statement advises the individual that the information provided is voluntary, and provides the consequences of choosing not to provide the information.

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.