PRIVACY IMPACT ASSESSMENT (PIA)

For the

NRL Personnel Demo Management System (PDMS)
Department of the Navy - ONR - 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 DON ID: 22931 DADMS ID: 86021
☐	**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: 007-000100284

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 DPR 34 DOD; OPM/GOVT-1; NM05000-2

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:

DPR 34 DOD: Defense Civilian Personnel Data System (November 15, 2010, 75 FR 69642).

5 U.S.C. 301, Department Regulations;
5 U.S.C. Chapter 11, Office of Personnel Management;
5 U.S.C. Chapter 13, Special Authority;
5 U.S.C. Chapter 29, Commissions, Oaths, Records, and Reports;
5 U.S.C. Chapter 31, Authority for Employment;
5 U.S.C. Chapter 33, Examination, Selection, and Placement;
5 U.S.C. Chapter 41, Training;
5 U.S.C. Chapter 43, Performance Appraisal;
5 U.S.C. Chapter 51, Classification;
5 U.S.C. Chapter 53, Pay Rates and Systems;
5 U.S.C. Chapter 55, Pay Administration;
5 U.S.C. Chapter 61, Hours of Work;
5 U.S.C. Chapter 63, Leave;
5 U.S.C. Chapter 72, Antidiscrimination; Right to Petition Congress;
5 U.S.C. Chapter 75, Adverse Actions;
5 U.S.C. Chapter 83, Retirement;

5 U.S.C. Chapter 99, Department of Defense National Security Personnel System;
5 U.S.C. 7201, Antidiscrimination Policy; minority recruitment program;
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness;
E. O. 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended;
29 CFR part 1614.601, EEO Group Statistics; and
E. O. 9397 (SSN), as amended.

OPM/GOVT-1: General Personnel Records. (April 27, 2000, 65 FR 24732)

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and
Executive Orders 9397, 9830, and 12107

NM05000-2: Program Management and Locator System (January 24, 2008, 73 FR 4194)

10 U.S.C. 5013, Secretary of the Navy; E.O. 9397 (SSN)

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.

Personnel Demo Management System (PDMS) is the Naval Research Laboratory (NRL) personnel demonstration project support system for the NRL as implemented under Federal Register Notice/Vol. 64, No.121 of June 24 1999. PDMS is an all inclusive data system that provides NRL employees and managers information required to make informed decisions in regards to performance appraisal, position classification, compensation adjustment decisions, requirement document creation, command drug testing and manpower management. Defense Civilian Personnel Data System (DCPDS) data is required to keep personnel records up-to-date for accurate decision making, reporting and overall support of the Naval Research Laboratory Navy Working Capital Fund operations.

PII data required for successful operation include the following:
Name
Social Security Number (SSN) (Full and truncated).
Citizenship
Race/Ethnicity
Gender
Legal Status
Date of Birth
Place of Birth
Home Address
Security Clearance
Other Names Used: Spouse Maiden Name
Other ID Number: Employee Number assign by DCPDS
Disability: Code indicating disability
Military Records: Are they a reservist, do they have veterans preference
Education Information: Education Level, Year of Degree, School of Degree
Employment Information: Previous employment, years of service

(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. PDMS system 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 the appropriate division head. Backups are monitored closely, and are encrypted. All PDMS users have gone through extensive background and employment investigations and annual Security and Information Assurance training. All PDMS screens and reports containing 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 PDMS computer rooms are secured with environmental alarms and key locks. Access to these locations is also limited to individuals who have a need to work in that area. NRL maintains an aggressive network monitoring program and PDMS is kept compliant with the DoD Information Assurance Vulnerability Management Program (IAVM). PDMS servers reside behind multiple firewalls.

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. Office of Civilian Human Resources - Philadelphia
NRL Management

☐ **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. Stacked Systems

52.224-1 Privacy Act Notification.

As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:
PRIVACY ACT NOTIFICATION (APR 1984)
The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.
(End of clause)
(R 7-2003.72 1975 NOV)
(R 1-1.327-5(b))

52.224-2 Privacy Act.

As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:
PRIVACY ACT (APR 1984)
(a) The Contractor agrees to--
(1) Comply with the Privacy Act of 1974 (the ACT) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract

specifically identifies--
(i) The systems of records; and
(ii) The design, development, or operation work that the contractor is to perform;
(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the design, development, or operation of a system of record on individuals that is subject to the Act; and
(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.
(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor and any employee of the Contractor is considered to be an employee of the agency.
(c) (1) 'Operation of a system of records', as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.
(2) 'Record,' as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.
(3) 'System of records on individuals,' as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

☐ **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.

PDMS does not collect PII directly from the individual.

(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.

PDMS does not collect PII directly from the individual.

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.

PDMS does not collect PII directly from the individual.

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.