PRIVACY IMPACT ASSESSMENT (PIA)

For the

Intellectual Property Management Information System (IPMIS)
Department of the Navy - Office of Naval Research (ONR)

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	8554
☐	**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 007-17-01-02-02-2982-00

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 N05870-1

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:

10 U.S.C. 5022, Office of Naval Research: duties.

Additional authorities:

SECNAV INST 5430.7Q, Assignment of Responsibilities and Authorities in the Office of the Secretary of the Navy: implements 10 U.S.C. 5022, requiring the Commander Naval Research to supervise, administer, and control activities relating to patents, inventions, trademarks, copyrights and royalty payments, and matters connected therewith.

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.

IPMIS is an enterprise intellectual property management system that enables Navy patent attorneys and their assistants to collect, process, and maintain information about inventions for which the U.S. Government (currently the Navy) owns the intellectual rights. The IPMIS allows users to create, view, and update cases and generate reports.

PII collected by IPMIS includes: Name (Navy patent attorneys and inventors (government and non-government)), citizenship, personal cell telephone number, home telephone number, personal e-mail address, mailing/home address, work mailing address, name and address of the company associated with the invention. Patent number is also collected.

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

The privacy risks are primarily computer hackers, state sponsored information warfare, disgruntled employees, and acts of nature (e.g., fire, flood, etc.).

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that IPMIS, with its collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.

All systems are vulnerable to "insider threats". IPMIS managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to IPMIS. These individuals have gone through extensive background and employment investigations.

The following controls are used to mitigate the risks:

a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.

b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes. This is accomplished by warning the user that IPMIS contains PII each time the user starts a new session and by encrypting the data whenever it is outside the ONR fire wall.

c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner. This is accomplished by making periodic data backups that can be used to recover 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. The Navy component offices have access to their own information in IPMIS. Additionally, access to all information is granted to ONR Headquarters personnel responsible for processing contracts associated with royalty payments.

☐ **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. Multiple contractors have access to PII for system development, maintenance, and operations. All contractor personnel at ONR must sign a Non-Disclosure Agreement for the protection of non-public information which includes the statement: "I agree to safeguard non-public information in accordance with relevant official rules and guidance, including but not limited to those contained in the National Industrial Security Procedures and Operations Manual (NISPOM), ONRINST 5211.2C (privacy), ONRINST 5239.10A (network security), ONRINST 5510.1A (ONR Security Manual), ONRINST 5570.1A (distribution statements), ONRINST 5570.2A (unclassified technical documents), and ONRINST 5720.4A (FOIA)." The agreement also includes the following definition: "Privacy-sensitive information includes Personally Identifiable Information (PII) and other information protected by the Privacy Act of 1974."

☐ **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.

The individual can object verbally and in writing to the collection of their PII. By not providing their PII, records related to inventions and patents would not be complete and difficult to track.

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

N/A

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.

Once an individual's PII is collected the information is only used to administer the Intellectual Property/Patent program.

(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.	Privacy Act Statement is provided to the individual at the time of collection: the authority for data collection; the principal purposes of the data collection; the routine uses of the data; and identifies what data disclosure is mandatory and what is voluntary and describes the effect on the individual if the data is not disclosed. Privacy Act statements are reviewed on a recurring basis and will be updated accordingly to reflect current Privacy Act policy and system requirements.

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.