PRIVACY IMPACT ASSESSMENT (PIA)

For the

FOIA AccessPro System
Office of Inspector General

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	4228
☐	**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 CIG-01

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.

The authority to collect information in this system derives from:

U.S. Code:
5 U.S.C. § 301, Regulations for the Government of the Department;
5 U.S.C § 552, the Freedom of Information Act;
5 U.S.C § 552a, the Privacy Act;
44 U.S.C. 3101 Records Management by Federal Agencies.

DoD Directives:
DoD Directive 5400.7, "DoD Freedom of Information Act (FOIA) Program," January 2, 2008, Change 1, July 28, 2011;
DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007, Change 1, September 1, 2011;
DoD Directive 5015.2, "DOD Records Management Program," March 6, 2000.

DoD IG Instructions:
IGDINST 5400.7, "Freedom of Information Act (FOIA) Program," April 16, 2010;
IGDINST 5400.11, "Privacy Act Program," January 29, 2010;
IGDINST 5015.2, "Records Management Program," November 7, 2007.

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.

Individuals submitting FOIA and/or Privacy Act requests to the Department of Defense Office of Inspector General FOIA Office provide PII with their request that can vary depending on the request. FOIA requesters generally submit their name(s), address, phone number, E-mail address. Privacy Act requesters provide the previously mentioned information and also the Date of Birth and Place of Birth of the individual for which records are sought, for positive identification purposes. This office does not request Social Security numbers nor does it require Social Security numbers to respond to Privacy Act requests.

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

Risk: There is a risk of unauthorized or inadvertent release of personal information, as well as unauthorized browsing of information by personnel for unofficial purposes.

Mitigation: To mitigate this risk, the FOIA Office has reduced access to authorized personnel to record level privacy and security on specifically identified case folders; Limited access to selected groups only to their particularized functions rather than the whole of the data; Implemented mandatory personnel security policies and procedures that require all personnel to be the subject of a favorable background investigation prior to being granted access to sensitive information systems; and Provided initial and follow-on privacy and security awareness training for each individual with access to FOIA and PA tracking systems.

Risk: There is a risk that malicious or inadvertent actions taken on a particular FOIA and/or PA request may not be traceable back to an individual.

Mitigation: To mitigate this risk, the FOIA Office has built in auditing controls for information technology systems whereby actions taken by a user on a case folder are tracked. This auditing feature maintains accountability of an action taken by an authorized user.

Risk: There is a risk that authorized individuals will have more permissions than required to perform their job function. This risk exists when any new user account is created.

Mitigation: To mitigate this risk, system administrators are responsible for reviewing the FOIA and PA programs permission matrix to ensure that programs are not allowing individual users' access to information that is not needed to complete necessary tasks, and that unauthorized individuals do not have access to information contained in the FOIA and PA programs.

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. Information is shared with FOIA POC of DoDIG Office(s) with responsive records

☒ **Other DoD Components.**

Specify. Information may be shared with FOIA POC of DoD Components with rights to review records or in order to respond to portions of the request.

☒ **Other Federal Agencies.**

Specify. Information may be shared with FOIA POC of agencies with rights to review records or in order to respond to portions of the request.

☒ **State and Local Agencies.**

Specify. In the instance State or Local Agency records are incorporated in to a file, the requester's information may be shared with that state or local agency for the purpose of providing sought records to the requester.

☐ **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.

Information provided to this Office for FOIA and Privacy Act requests is done voluntarily. The requesters may choose not to file a FOIA or Privacy Act request. The requester may choose not to provide any PII when making an initial request for records, however without it this Office may not be able to properly respond to requests.

(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.

Individuals can give consent to using their PII by providing the information in the initial request for records. The PII that is provided by the requester will only be used to locate and verify that the records sought pertain to the requester, and the requester has a right to access the records.

(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.