PRIVACY IMPACT ASSESSMENT (PIA)

For the

Arms and Arms CA
HRD

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: 7554
- ☐ **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 007-97-01-03-02-1915-00

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 DWHS P29

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.

Per the Privacy Act SORN, the authorities to collect information are:

5 U.S.C. 301, Departmental Regulations; and Executive Order 12356, Executive Order 10450, Executive Order 9397.

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.

The Adjudications Records and Management System (ARMS) and ARMS Customer Access are two web-enabled applications. ARMS enables the WHS Consolidated Adjudications Facility (CAF) to track and manage adjudications workflow, data, correspondence and reports for the Office of the Secretary of Defense and all Department of Defense (DoD) agencies and activities supported by the WHS CAF. ARMS Customer Access provides the headquarters security offices of the primary agencies supported by the WHS CAF with limited "read-only" information pertaining to the status of cases for employees of the specific agency. Personal information stored and managed through these applications is used by the WHS CAF to administer its adjudicative responsibilities, track case action, document issues, and record determinations for security clearance and position of public trust determinations for civilian employees and applicants of the Office of the Secretary of Defense, all Department of Defense (DoD) agencies and activities (minus the intelligence agencies), Congressional Staff, Congressional Budget Office, and United States Capitol Police.

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

The privacy risks associated with the PII collected are the unauthorized release of PII data. These risks are addressed by protecting the data collection resource with strong SSL encryption, programmatically restricting the system from releasing PII data through its interfaces, through SSL encryption with CAC of PII released to partner agencies under the routine use guidelines authorized in the Privacy Act System Of Record Notice (SORN), through periodic Information Assurance training of personnel with access to the PII, and through access control restricted by CAC to internal network personnel whose job functions require access to PII. Moreover, those authorized security personnel with access to the ARMS and ARMS Customer Access applications have a favorably adjudicated Single Scope Background Investigation.

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. Washington Headquarters Services customer agencies within DoD

☐ **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.

At the time individuals initiate the personnel security process they are requested by their employing agency's security office to execute the Office of Management and Budget approved, Office of Personnel Management administered, Standard Form 85, Standard Form 85P, or Standard Form 86 as determined by the purpose of their investigation. These forms inform individuals that providing the requested personal information is voluntary and the disclosure of information and routine uses are explained. When an individual completes any of these forms and signs the applicable authorizations for release of information the individual is consenting to the collection of PII. Conversely, the individual can object to the collection of PII by not completing these forms and signing the applicable authorizations of release, at which time the process ceases.

(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.

The individual is able to object, as cited in 2.i.(1); however, once the information is collected the individual is unable to pick and choose how the information will be used during the conduct of the adjudication for access to classified information and/or occupancy of a position of public trust.

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.

All applicant records in ARMS, which are managed by authorized WHS CAF staff, have the following regulatory notices as part of the personnel record:

Social Security Number: A social security number is requested under the authority of Executive Order 9397 to uniquely identify records of applicants who may have the same name. Also, as allowed by law or presidential directive, a social security number is used to map candidates' records to their corresponding personnel files and assign a unique ARMS record to a case.

Privacy Act - Privacy Act notice (DWHSP29): The information requested here is used to manage candidate information and adjudicative decisions.

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.