PRIVACY IMPACT ASSESSMENT (PIA)

For the

DTMO Workforce Assessment
Defense Travel Management Office

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: 12784
- ☐ **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 000004499

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 DHRA 13 DoD

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.

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; Department of Defense (DoD) Directive 5100.87, Department of Defense Human Resources Activity; DoD Instruction 5154.31, Commercial Travel Management.

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.

To administer an assessment that will enable the analysis of workforce capabilities and competency gaps within the DTMO organization. The assessment will aid in identifying personnel with competencies necessary to manage programs assigned to the DTMO in DoD Instruction 5154.31 and meet organizational goals. Data collected will allow for the development of strategies to address human capital needs, close competency gaps, and ensure personnel are appropriately aligned within the DTMO's organizational structure.

Types of personal information collected include full name, current job position and grade, work experience, leadership experience, future job aspirations, subject matter expertise, job-related skills, training received, degrees earned and fields of study, professional licenses and certifications.

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

Risks associated with unauthorized disclosure are minimal. The information collected is what can be found on a typical resume. While the risk is small, all administrative, physical, and technical controls (secured datacenter, encryption, intrusion detection, access controls, etc.) employed by the DTMO for the protection of Privacy Act data have been applied to this data collection.
Records are stored on secure military installations. Physical controls include use of visitor registration and identification badges, electronic key card access, and closed-circuit television monitoring. Technical controls including intrusion detection systems, secure socket layer encryption, firewalls, and virtual private networks protect the data in transit and at rest. Physical and electronic access is limited to individuals who are properly screened and cleared on a need-to-know basis in the performance of their official duties. Usernames and passwords and Common Access Cards (CACs), in addition to role-based access controls are used to control access to the systems data. Procedures are in place to deter and detect browsing and unauthorized access including periodic security audits and monitoring of users' security practices. Backups are stored on encrypted media and secured off-site.

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.

☐ **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.

Personnel may elect not to fill out the questionnaire if they object to the collection of their PII.

(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.

Employees are presented with an informational page that describes the intended uses of the data. If they object to specific uses, they can elect not to participate in the questionnaire and submit a statement of objection to their DTMO supervisor.

(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.

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; Department of Defense Directive 5100.87, Department of Defense Human Resources Activity; Department of Defense Instruction 5154.31, Commercial Travel Management.

PRINCIPAL PURPOSE(S): To administer an assessment that will enable the analysis of workforce capabilities and competency gaps within the DTMO organization. The assessment will aid in identifying personnel with competencies necessary to manage programs assigned to the DTMO in DoD Instruction 5154.31 and meet organizational goals. Data collected will allow for the development of strategies to address human capital needs, close competency gaps, and ensure personnel are appropriately aligned within the DTMO's organizational structure. [add link to SORN when published.]

ROUTINE USE(S): The DoD Blanket Routine Uses found at http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx may also apply to this collection.

DISCLOSURE: Voluntary. However, failure to provide requested information may limit DTMO's ability to identify personnel with competencies necessary to manage programs and meet organizational goals.

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.