PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Competency Assessment Tool (DCAT)
Defense Civilian Personnel Advisory Service (DCPAS)

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	15016
☐	**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 OPM/GOVT-6: Personnel Research and Test Validation Records

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.

5 U.S.C. 1301, 1303, and 4702 (Governing sources for corresponding Privacy Act SORN); 10 U.S.C. 115b; DoDI 1400.25, Volume 250, Civilian Strategic Human Capital Planning (SHCP), November 18, 2008.

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 Defense Competency Assessment Tool (DCAT) will be used to identify current and future competency requirements of the civilian DoD workforce based on the near-term and long-term organizational goals. The system will be used to determine the importance of identified competencies for each position, identify current competency needs, and identify future competency needs within the civilian workforce at DoD. The tool will provide a repository for identified competencies divided into five tiers, allow supervisors and employees to complete a competency profile and validate competency importance, document proficiency assessments by supervisors and employees DoD-wide, and provide competency gap reporting.

DCAT will collect and store the following data elements: name, DOD ID number (EDIPI), occupational series, grade, organization name, work address, work email, supervisory status code, pay status code, and responses to competency assessment questionnaires.

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

All systems are at risk to "outside threats" such as computer hackers, and state-sponsored information warfare. There are risks that DCAT, with its collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.

In addition, all systems are vulnerable to "insideir threats." DCAT administrators will be 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, and what level of access they should have to DCAT. These individuals have gone through extensive background and employment investigations.

A few risk mitigation strategies are listed below, but are not limited to:

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 user interface features (such as buttons and menu items) are enable for the user currently logged on.

b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, or entities.

c) Integrity. This ensures that data has not been created, altered or destroyed in an unauthorized manner.

d) Audits. This includes review and examination or records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.

e) Training. Security training is provided on a regular basis to keep users alert to the security requirements.

f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. An internal policy is set in place to ensure that there are always no less than two users present at a time when privileged information is being retrieved. Since the server and data reside within the DoD environment, the strict security measures set by the establishment are always followed.

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. Defense Civilian Personnel Advisory Service (DCPAS)

☒ **Other DoD Components.**

Specify. Air Force, Navy, Army, Fourth Estate

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. All contractors are cleared for and trained in PII protection. Contracts require protection in accordance with 5CFR522a.

☐ **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.

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

DCAT receives PII from an extract from the Defense Civilian Personnel Data System (DCPDS). Participation in the competency assessment itself is voluntary, but DCAT will still include a record related to each DoD civilian employee.

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.

DoD requires all civilian employees to use DCAT for competency assessment activities so that it can meet congressionally mandated reporting requirements as indicated in NDAA 2010.

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: 5 U.S.C. 1301, 1303, and 4702; 10 U.S.C. 115b; and DoDI 1400.25, Volume 250, Civilian Strategic Human Capital Planning (SHCP).

PURPOSE: The information from this electronic competency assessment will be used by DoD for workforce planning and training and development purposes. Employees will rate their proficiency in a set of competencies aligned with their occupational series. Supervisors will assess their employee's proficiency level in each of these competencies and identify the target proficiency levels for the position. Supervisors and employees are encouraged to discuss the results to plan for future training and development opportunities

ROUTINE USE(S): The DoD 'Blanket Routine Uses' found at http://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.html may apply.

DISCLOSURE: Voluntary. No individual administrative decisions are made based on this information; however, your responses will allow the DoD to better develop the needs of its civilian workforce.

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.