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-1: General Personnel 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. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107.
(Governing sources for corresponding Privacy Act SORN.)

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 ultimately be used to determine the importance level 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 5 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.

Examples of PII collected include: Name, Gender, and Birth Date.

(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, disgruntled employees 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 "insider 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 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.

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 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.

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

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 the 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.

The Privacy Act Statement will be delivered in electronic format on the web application when the user enters the web site.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	□ Other Names Used	□ Social Security Number (SSN)
□ Truncated SSN	□ Driver's License	□ Other ID Number
□ Citizenship	□ Legal Status	☒ Gender
□ Race/Ethnicity	☒ Birth Date	□ Place of Birth
□ Personal Cell Telephone Number	□ Home Telephone Number	□ Personal Email Address
□ Mailing/Home Address	□ Religious Preference	□ Security Clearance
□ Mother's Maiden Name	□ Mother's Middle Name	□ Spouse Information
□ Marital Status	□ Biometrics	□ Child Information
□ Financial Information	□ Medical Information	□ Disability Information
□ Law Enforcement Information	☒ Employment Information	☒ Military Records
□ Emergency Contact	☒ Education Information	□ Other

If "Other," specify or explain any PII grouping selected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

There are three potential sources of data: Defense Civilian Personnel Data System (DCPDS), authorized administrators within the application, or the end users.

(3) How will the information be collected? Indicate all that apply.

☐ **Paper Form**

☐ **Telephone Interview**

☐ **Email**

☒ **Information Sharing - System to System**

☐ **Other**

☐ **Face-to-Face Contact**

☐ **Fax**

☒ **Web Site**

Some information will be imported from DCPDS data extracts. Other information could be entered by an approved administrator or by the user. All information is gathered electronically.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Personal information such as name, gender, and birth date is used for verification and identification purposes. Other experience related information such as Employment Information and Education Information is used as part of the competency repository for each employee.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

As mentioned previously, PII is collected for verification and identification purposes, as well as inputs into the competency management process.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☒ **Contractors**

☐ **Other**

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☐ **Security Guards**

☒ **Identification Badges**

☒ **Key Cards**

☐ **Safes**

☒ **Cipher Locks**

☐ **Combination Locks**

☐ **Closed Circuit TV (CCTV)**

☒ **Other**

Access to Computing Facilities: Only those individuals that are authorized to be in the computing facilities will have access to the PII.

Physical Protection of Facilities: The facilities will have physical protection - such as door locks and door access codes.

Storage: The storage area for the equipment and hardware will be secure - locks and access codes will be in place.

Visitor Control to Computing Facilities: All visitors will be monitored and escorted in the facilities. Unauthorized guests are prohibited.

(2) Technical Controls. Indicate all that apply.

☐ **User Identification**

☐ **Password**

☐ **Intrusion Detection System (IDS)**

☒ **Encryption**

☐ **External Certificate Authority (CA) Certificate**

☐ **Other**

☐ **Biometrics**

☒ **Firewall**

☒ **Virtual Private Network (VPN)**

☒ **DoD Public Key Infrastructure Certificates**

☒ **Common Access Card (CAC)**

(3) Administrative Controls. Indicate all that apply.

☒ **Periodic Security Audits**

☒ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

□ **Other**

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☒	**Authorization to Operate (ATO)**	**Date Granted:**	Pending Development
□	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
□	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
□	**Interim Authorization to Test (IATT)**	**Date Granted:**	

□ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection: Member PII information is collected through scheduled interface pulls from authoritative data sources (ADS) through a secure connection; VPN, HTTPS, and SSL. There is no user activity during this process. Sensitive PII (SSN) will be encrypted using a strong compliant algorithm.

Use, Retention, and Processing: Authorized personnel who are authenticated can access their own information for competency management purposes. Individuals with the "need to know" will have access to a member's PII information but will be limited on screen and print. Additionally, database keys will be used to retrieve information on an individual.

Disclosure: No other personnel other than the individual and persons with a "need to know" can access a member's PII information unless permission is granted from the individual in writing or authorizing an individual to

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

N/A

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Any identified privacy risks are mitigated in the same way that all risks are mitigated as described in Section 2.G.2.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	WHITE.FRAN.C.1281288233 Digitally signed by WHITE.FRAN.C.1281288233 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=WHITE.FRAN.C.1281288233 Date: 2012.07.25 13:18:43 -04'00'
Name:	Fran White
Title:	Program Manager
Organization:	Defense Civilian Personnel Advisory Service (DCPAS) - Enterprise Human Resources Information Systems (EHRIS)
Work Telephone Number:	571-372-2223
DSN:	372-2223
Email Address:	fran.white@cpms.osd.mil
Date of Review:	
Other Official Signature (to be used at Component discretion)	LEPORE.MARY BETH.NMI.1072445585 Digitally signed by LEPORE.MARY BETH.NMI.1072445585 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=LEPORE.MARY BETH.NMI.1072445585 Date: 2012.08.06 08:50:41 -04'00'
Name:	Mary Beth Lepore
Title:	Functional Manager
Organization:	Defense Civilian Personnel Advisory Service (DCPAS) - Strategic Human Capital Planning Division (SHCPD)
Work Telephone Number:	571 372 2119
DSN:	372 2119
Email Address:	mary.lepore@cpms.osd.mil
Date of Review:	

Other Official Signature (to be used at Component discretion)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Component Senior Information Assurance Officer Signature or Designee	DESANTO.SARAH.ANN.1121873679 Digitally signed by DESANTO.SARAH.ANN.1121873679 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=DESANTO.SARAH.ANN.1121873679 Date: 2012.08.16 10:13:56 -04'00'
Name:	Sally DeSanto
Title:	Senior Information Assurance Officer (SIAO)
Organization:	Personnel & Readiness Information Management
Work Telephone Number:	703-696-8710
DSN:	426-8710
Email Address:	sally.desanto@osd.pentagon.mil
Date of Review:	
Component Privacy Officer Signature	RODGERS.DEBORAH.A.1016613653 Digitally signed by RODGERS.DEBORAH.A.1016613653 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=RODGERS.DEBORAH.A.1016613653 Date: 2012.08.06 15:39:41 -04'00'
Name:	Deborah Rodgers
Title:	DCPAS Privacy Officer
Organization:	DCPAS Corporate Support Division
Work Telephone Number:	571 372 2163
DSN:	372 2163
Email Address:	Deborah.Rodgers@cpms.osd.mil
Date of Review:	

Component CIO Signature (Reviewing Official)	LINCECUM.MICHAEL.J.1065265326 Digitally signed by LINCECUM.MICHAEL.J.1065265326 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=LINCECUM.MICHAEL.J.1065265326 Date: 2012.08.19 10:01:15 -04'00'
Name:	Michael Lincecum
Title:	Chief Information Officer (CIO)
Organization:	Defense Human Resource Activity (DHRA)
Work Telephone Number:	703.696.8710
DSN:	
Email Address:	michael.lincecum@osd.pentagon.mil
Date of Review:	

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.