PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Defense Civilian Human Resource Management System (DCHRMS)

2. DOD COMPONENT NAME:

Defense Human Resources Activity

Defense Civilian Personnel Advisory Service (DCPAS)

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [ ] Existing Electronic Collection
- [x] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

To maintain a system of records that provides human resource information and system support for the Department of Defense (DoD) civilian workforce worldwide that manages the human resources processing and reporting, including position, compensation and benefits, and performance management, as well as create efficiencies in Human Capital Management.

Position authorization and control information; position data and performance elements; personnel data and projected suspense information for personnel actions; pay, benefits, and entitlements data. Historical information on employees, including job experience, education, training, and training transaction data; performance plans, interim appraisals, final appraisals, closeouts and ratings; professional accounting or other certifications or licenses; awards information and merit promotion information; separation and retirement data; civilian deployment information and adverse and disciplinary action data. Personal information including Social Security Number (SSN), DoD identification number (DoD ID), employee number, emergency contact information (name, home/work/cell phone number, email address), employee email address, employee phone numbers to include home, work, pager, fax and mobile; ethnicity; disability code; and foreign language capability. In addition, the Corporate Management Information System data, which houses employee historical assignment, position, and personnel actions data, will be maintained for historical purposes, however, the data will not be refreshed.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Mission-related use

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

The application is used on a voluntary basis, but is required to process all human resources, position management, compensation and benefits, and performance management requests.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

Once an individual voluntarily provides their information, it will be used to process all human resources, position management, compensation and benefits, and performance management requests, as required.

g. **When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided.** *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

Authorities: 5 U.S.C. Chapter 11, Office of Personnel Management; 5 U.S.C. Chapter 13, Special Authority; 5 U.S.C. Chapter 29, Commissions, Oaths, Records, and Reports; 5 U.S.C. Chapter 31, Authority for Employment; 5 U.S.C. Chapter 33, Examination, Selection, and Placement; 5 U.S.C. Chapter 41, Training; 5 U.S.C. Chapter 43, Performance Appraisal; 5 U.S.C. Chapter 51, Classification; 5 U.S.C. Chapter 53, Pay Rates and Systems; 5 U.S.C. Chapter 55, Pay Administration; 5 U.S.C. Chapter 61, Hours of Work; 5 U.S.C. Chapter 63, Leave; 5 U.S.C. Chapter 72, Antidiscrimination; Right to Petition Congress; 5 U.S.C. 7201, Antidiscrimination Policy; minority recruitment program; 5 U.S.C. Chapter 75, Adverse Actions; 5 U.S.C. Chapter 83, Retirement; 5 U.S.C. Chapter 84, Federal Employees' Retirement System, Antidiscrimination Policy; minority recruitment program; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; E. O. 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended; 29 CFR part 1614.601, EEO Group Statistics; and E. O. 9397 (SSN), as amended.

Principal Purposes: To maintain a system of records that provides human resource information and system support for the Department of Defense (DoD) civilian workforce worldwide that manages the human resources processing and reporting, including position, compensation and benefits, and performance management, as well as create efficiencies in Human Capital Management.

Routine Uses: To the Equal Employment Opportunity Commission (EEOC) for the purpose of providing Equal Employment Opportunity group statistics in accordance with 29 CFR part 1614.601, EEO Group Statistics.

To the Office of Personnel Management (OPM) for the purpose of addressing civilian pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

Additional routine uses may be found in the applicable system of records notice DHRA 23 DoD, Defense Civilian Human Resource Management System (DCHRMS) at: TBD

Disclosure: Voluntary. However, failure to provide or update your information may require manual human resources processing or the absence of some information in your HR record.

h. **With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component?** *(Check all that apply)*

☒ Within the DoD Component	Specify.	DMDC
☒ Other DoD Components	Specify.	DoD Acquisition Office; Air Force; DLA; DFAS; DHA; All other DoD Serviced Components
☒ Other Federal Agencies	Specify.	To the Equal Employment Opportunity Commission (EEOC) for the purpose of providing Equal Employment Opportunity group statistics in accordance with 29 CFR part 1614.601, EEO Group Statistics. To the Office of Personnel Management (OPM) for the purpose of addressing civilian pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.
☐ State and Local Agencies	Specify.	
☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Oracle Corporation; Leidos Corporation. Included contract clauses: 52.224-1 Privacy Act Notification APR 1984 52.224-2 Privacy Act APR 1984

[X] Other *(e.g., commercial providers, colleges).* Specify. To educational institutions and commercial training providers for the purpose of selecting and registering applicants approved by a DoD component to attend a specified program, and, when applicable, to provide for payment.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

[X] Individuals
[X] Databases
[X] Existing DoD Information Systems
[ ] Commercial Systems
[ ] Other Federal Information Systems

Joint Personnel Adjudication System; Fourth Estate Manpower Tracking System; Defense Civilian Payroll System; the Air Force Manpower Programming and Execution System; NAF Payroll; Interactive Voice Recognition System (IVRS); USA Staffing

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

[ ] E-mail
[X] Official Form (*Enter Form Number(s) in the box below)*
[ ] Face-to-Face Contact
[ ] Paper
[ ] Fax
[ ] Telephone Interview
[X] Information Sharing - System to System
[X] Website/E-Form
[X] Other *(If Other, enter the information in the box below)*

Prospective employee generated resume; applicant record; SF 181, Ethnicity and Race Identification; SF 256, Self-Identification of Disability; SF 144, Statement of Prior Federal Service; SF 181, "Ethnicity and Race Identification"; SF 256, "Self-Identification of Disability"; SF 144, "Statement of Prior Federal Service"; OF 306, "Declaration for Federal Employment"; DD 214, "Certificate of Release or Discharge from Active Duty"; SF 813, "Verification of a Military Retiree's Service In NonWartime Campaigns or Expeditions"; SF 15, "Application for 10-Point Veteran Preference"; SF 52, "Request for Personnel Action"; SF 50, "Notification of Personnel Action"; SF 61, "Appointment Affidavit"; DD X739, "Civilian Employee's Military Reserve, Guard, or Retiree Data,"; DD 2888, "DoD Critical Acquisition Position Service Agreement"; DD 2889, "DoD Critical Acquisition Position Service Agreement Key Leadership Position (KLP)"; DD 2365, "DoD Expeditionary Civilian Agreement: Emergency-Essential Positions and Non-Combat Essential Positions"; DD 3031, "Department of Defense Senior Executive Service Probation Period"; SF 2809, "Employees' Health Benefits Election"; SF 2817, "Federal Employees' Retirement System Election"; SF 75, "Request for Preliminary Employment Data"; employee or supervisor generated training requests; human resources generated records; employee generated data recorded as self-certified; other employee or supervisor generated records; and employee completed training data provided by respective Component agencies.

k. 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 must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier DHRA 23 DoD

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N1-330-10-2

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Destroy inactive personnel records when 25 years old.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

5 U.S.C. Chapter 11, Office of Personnel Management; 5 U.S.C. Chapter 13, Special Authority; 5 U.S.C. Chapter 29, Commissions, Oaths, Records, and Reports; 5 U.S.C. Chapter 31, Authority for Employment; 5 U.S.C. Chapter 33, Examination, Selection, and Placement; 5 U.S.C. Chapter 41, Training; 5 U.S.C. Chapter 43, Performance Appraisal; 5 U.S.C. Chapter 51, Classification; 5 U.S.C. Chapter 53, Pay Rates and Systems; 5 U.S.C. Chapter 55, Pay Administration; 5 U.S.C. Chapter 61, Hours of Work; 5 U.S.C. Chapter 63, Leave; 5 U.S.C. Chapter 72, Antidiscrimination; Right to Petition Congress; 5 U.S.C. Chapter 75, Adverse Actions; 5 U.S.C. Chapter 83, Retirement; 5 U.S.C. Chapter 84, Federal Employees' Retirement System; 5 U.S.C. 7201, Antidiscrimination Policy; minority recruitment program; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; E. O. 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended; 29 CFR part 1614.601, EEO Group Statistics; and E. O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

While the system maintains information on members of the public, it is not the initial collection point for that data.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

☐ Biometrics	☒ Birth Date	☐ Child Information
☒ Citizenship	☒ Disability Information	☒ DoD ID Number
☐ Driver's License	☒ Education Information	☒ Emergency Contact
☒ Employment Information	☒ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☒ Mailing/Home Address	☒ Marital Status	☐ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☐ Official Duty Address	☐ Official Duty Telephone Phone	☒ Other ID Number
☐ Passport Information	☒ Personal E-mail Address	☐ Photo
☒ Place of Birth	☒ Position/Title	☐ Protected Health Information (PHI)[1]
☒ Race/Ethnicity	☒ Rank/Grade	☐ Religious Preference
☐ Records	☒ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☒ If Other, enter the information in the box below	

Spouse

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☒ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

Signed by Ms. Katrina Logan, DHRA Senior Component Official for Privacy, February 17, 2019
Approved by Ms. Cindy Allard, Director, Defense Privacy, Civil Liberties, and Transparency Division, April 15, 2019

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Collection of the SSN for this system meets acceptable use (8), Computer Matching. In compliance with Office of Personnel Management (OPM) requirements/standards for electronic maintenance and processing of personnel records, the SSN is collected in DCHRMS. DCHRMS also exports data to other systems, such as the OPM Enterprise Human Resources Integration, Electronic Official Personnel Folder, OPM's USAJOBS Recruitment Tool and other Federal agency systems to process personnel actions and provide human resources information and system support for the management and operations of DoD civilian workforce.

Acceptable use (5), Confirmation of Employment Eligibility, applies as DCHRMS is the mechanism which provides sponsorship and verifies eligibility for a Common Access Card (CAC) and DoD ID Number for new employees. DCHRMS, as the system of record, interfaces with DMDC to provide pertinent employee data which is transmitted to the DoD Person Data Repository, better known as the Defense Enrollment Eligibility Reporting System, to initiate the issuance of a DoD CAC and assignment of an electronic data interchange personal identifier, also known as DoD ID Number.

The Legacy System Interface, acceptable use (11), addresses DCHRMS interfaces with the Defense Civilian Payroll System, the Defense Finance and Accounting Services DoD payroll system that records, processes, maintains and reports civilian employee data, pay entitlement and benefits elections. DCHRMS is the catalyst, via the processing of personnel transactions affecting pay and benefits, which initiates requisite financial transactions to occur in the DCPS. The interface between DCHRMS and DCPS is constrained by DCPS and its limited capability, as a legacy system, which cannot accommodate the ten-digit DoD ID number and must continue the use of the SSN.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

Safeguards are in place to protect all personally identifiable information maintained within the system, in accordance with the Privacy Act of 1974 and DoD 5400.11-R, "Department of Defense Privacy Program."

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

At such time as the systems with interface with and export data from DCHRMS no longer require SSNs, the identifier will be removed from the system.

b. What is the PII confidentiality impact level[2]? ☐ Low ☒ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- ☒ Cipher Locks
- ☐ Combination Locks
- ☒ Key Cards
- ☒ Security Guards
- ☒ Closed Circuit TV (CCTV)
- ☒ Identification Badges
- ☐ Safes
- ☒ If Other, enter the information in the box below

Biometric access systems, multiple layers of locked access control doors and mantraps, and physical intrusion alarms.

(2) Administrative Controls. *(Check all that apply)*

- ☒ Backups Secured Off-site
- ☒ Encryption of Backups
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☒ Periodic Security Audits
- ☐ Regular Monitoring of Users' Security Practices
- ☐ If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- ☐ Biometrics
- ☒ Encryption of Data at Rest
- ☒ Firewall
- ☒ Role-Based Access Controls
- ☒ Virtual Private Network (VPN)
- ☒ Common Access Card (CAC)
- ☒ Encryption of Data in Transit
- ☒ Intrusion Detection System (IDS)
- ☐ Used Only for Privileged (Elevated Roles)
- ☒ If Other, enter the information in the box below
- ☒ DoD Public Key Infrastructure Certificates
- ☐ External Certificate Authority Certificates
- ☒ Least Privilege Access
- ☒ User Identification and Password

Two-factor authentication
Each customer must provide an IdM/IdP and authenticate their CACs, the customer IdM/IdP would pass a SAML assertion to Oracle for Single Sign ON.
Oracle utilizes privilege use management software to authorize, audit, control, and monitor all privileged functions. Those functions are audited and ingested by Oracle's SIEM

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?