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:

Survey Database

2. DOD COMPONENT NAME:

Defense Human Resources Activity

3. PIA APPROVAL DATE:

12/18/20

Office of People Analytics (OPA)

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
- [x] Existing Electronic Collection
- [ ] 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.

OPA is establishing a repository of existing data sources for research and analytical purposes. The data is used to provide the DoD with fast, accurate assessments of the attitudes and opinions of the entire DoD community in order to evaluate existing programs/policies, establish baseline measures before implementing new programs/policies, and monitor progress of programs/policies and their effects on the total force. The data is also used to support manpower research sponsored by DoD and the military services. Survey results provide direct feedback on key Departmental strategic indicators. These indicators provide primary data on personnel career plans, discrimination, sexual harassment/assault, suicide ideation, retention decisions, morale, and commitment, and historically provide the ability to evaluate the impact of policies and programs with regard to readiness and retention. The surveys also serve as benchmarks by which senior DoD officials can track trends over time.

Responses from joint-Service surveys that assess the attitudes, opinions, and/or experiences of the entire DoD community on topics related to general quality of life, programs, policies, readiness, retention, gender relations, and race/ethnic discrimination. Responses include but are not limited to: attitudes and opinions on satisfaction with leadership, reasons to join the military, military way of life, use of programs and services, and experiences related to sexual harassment, sexual assault, race/ethic discrimination, hazing, bullying, and retaliation.

With the exception to the Defense Equal Opportunity Climate Survey (DEOCS), all survey respondents are assigned a survey ID, a unique identifier, which allows for sorting and analyzing the results. In the DEOCS database, OPA uses EDIPI as the unique identifier to produce higher aggregations of DEOCS weighting and estimation (as approved by the IRB). EDIPI and email addresses might also be collected from a limited number of DEOCS participants. This collection occurs when the survey participant's email is not on the administrative file, and OPA collects EDIPI from the survey participant to verify that they are part of the military community. For spouse surveys, email addresses are not available on the administrative record files. To gain efficiency in surveying military spouses, OPA will use a media campaign that encourages military spouses to voluntarily submit their personal email addresses on the OPA survey portal. Email addresses collected will be used for future OPA spouse surveys; emails will never be stored with the survey responses.

To protect survey respondents, OPA does not store DoD ID numbers or other direct identifiers in the same database as survey responses. Instead, OPA maintains a bridge file that contains DoD ID numbers and the random Survey ID numbers that reside on OPA survey response datasets. This bridge file allows OPA to link survey datasets to either 1) DoD administrative data, or 2) other OPA survey data to support research. Access to the bridge files is limited to a very small set of OPA staff that can provide these linkages.

The categories of records for DoD administrative data includes: Name, gender, marital status, birth date, race/ethnicity, home address, email, work and home/cell phone numbers, citizenship, education information; employment information (military or civilian organization), rank, date of rank, date entered service, pay grade, occupational series, duty position; child information; DoD Identification Number,Other ID

number, and educational attainment on military service members, spouses and their dependents and civilians.

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 individual does not have the ability to object to the collection of their data in the Survey Database, since this system is not the initial point of collection. The individual would have to opt out at the source system for their PII data not to be collected in the Survey Database.

EDIPI and email addresses will be collected from a limited number of survey participants. For unit surveys, when the survey participant's email is not on the administrative file, OPA will collect EDIPI from the survey participant to verify that they are part of the military community. For spouse surveys, email addresses are not available on the administrative record files. To gain efficiency in surveying military spouses, OPA will use a media campaign that encourages military spouses to voluntarily submit their personal email addresses on the OPA survey portal. Email addresses collected will be used for future OPA spouse surveys. So when the individual chooses to provide their email address they are implicitly consenting to the specific use.

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.

The individual does not control the specific use of the PII data once collected into the Survey Database. All data within the Survey Database is initially captured in other systems of record.

EDIPI and email addresses will be collected from a limited number of survey participants. For unit surveys, when the survey participant's email is not on the administrative file, OPA will collect EDIPI from the survey participant to verify that they are part of the military community. For spouse surveys, email addresses are not available on the administrative record files. To gain efficiency in surveying military spouses, OPA will use a media campaign that encourages military spouses to voluntarily submit their personal email addresses on the OPA survey portal. Email addresses collected will be used for future OPA spouse surveys. So when the individual chooses to provide their email address they are implicitly consenting to the specific use.

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 [X] Not Applicable

The Survey Database does not directly collect PII from individual users. However, EDIPI and email addresses will be collected from a limited number of survey participants. For unit surveys, when the survey participant's email is not on the administrative file, OPA will collect EDIPI from the survey participant to verify that they are part of the military community.

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.	
[X] Other DoD Components	Specify.	OUSD P&R, Air Force, Air Force Reserve, Air National Guard, Air Force Academy, Army, Army National Guard, Army Academy/ROTC, Army Reserve, Marine Corps, Marine Corps Reserve, Navy, Naval Academy, and Navy Reserve.
[X] Other Federal Agencies	Specify.	Coast Guard, Coast Guard Reserve, Coast Guard Academy, Federal Reserve Board, GAO, USDA
[ ] 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.	OPA's Survey Contractors (currently DRC corporation for data collection and Fors Marsh Group for data analysis) have access to these data. The contract includes the Privacy Act clause of the Federal Acquisition Regulation (FAR), specifically FAR 52.224-2, under which the contractor/subcontractor agrees to comply with the requirements of the Privacy Act and DoD rules and regulations issued under the Act. This contract provision also treats the contractor/subcontractor as an employee of DoD for purposes of the Privacy Act, and is thus subject to possible criminal penalties if the Act is violated. The contract also incorporates FAR 52.239-1, Privacy and Security safeguards, which includes a notification requirement if new or unanticipated threats or hazards are discovered, or if existing safeguards cease to function.
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

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

- ☒ Individuals
- ☒ Existing DoD Information Systems
- ☐ Other Federal Information Systems
- ☒ Databases
- ☐ Commercial Systems

For existing data, we will not have direct contact. For future collections, we will contact individuals, via web, paper, phone, in person surveys.

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

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

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier DMDC 08

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. N1-330-03-001

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

(3) Retention Instructions.

Master file, system documentation, codebooks, record layouts, and other system documentation. Permanent, Cut off on completion of the report for the DoD office requiring the creation of the report. Transfer master file and system documentation to NARA at cutoff in accordance with standards of 36 CFR 1228.270 and 36 CFR 1234.

Hard copy survey questionnaires (inputs/source records).Temporary, Destroy after computer records have been created and validated.

Summary reports (electronic or paper). Temporary, Delete/destroy when no longer needed for operational purposes

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.

10 USC 136, Under Secretary of Defense for Personnel and Readiness;10 USC 481, Racial and Ethnic Issues; Gender Issues: Surveys; 10 U.S.C. 503(a), Enlistments: recruiting campaigns;10 USC 1782, Surveys of Military Families;10 USC 2358, Research and Development Projects; Section 572 of PL 112–239, National Defense Authorization Act for Fiscal Year 2013, DoD Instruction (DoDI) 1100.13, DoD Surveys; DoDI 1332.14, Enlisted Administrative Separations; DoDI 1332.30, Commissioned Officer Administrative Separations; DoDI 5505.18, Investigation of Adult Sexual Assault in the Department of Defense; DoDI 6945.02, Sexual Assault Prevention and Response (SAPR) Program Procedures; and Executive Order (EO) 9397 (SSN).

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.

Exempt from OMB approval in accordance with 10 U.S.C. 503(a), (Subchapter I of chapter 35 of title 44 shall not apply).

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	

EDIPI and email addresses will be collected from a limited number of survey participants. For unit surveys (DEOCS), when the survey participant's email is not on the administrative file, OPA will collect EDIPI from the survey participant to verify that they are part of the military community. For spouse surveys, email addresses are not available on the administrative record files. To gain efficiency in surveying military spouses, OPA will use a media campaign that encourages military spouses to voluntarily submit their personal email addresses on the OPA survey portal. Email addresses collected will be used for future OPA spouse surveys. Personal emails are sometimes purchased by Experian.

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.

SSN Justification Memoranda are in place at the initial point of collection. Data is identified by the system administrators before being accessed by OPA researchers and analysts.

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

(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".

(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

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)*

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

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

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

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

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

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