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:

SECNAV 12306/1 Confirmation of Reasonable Accommodation Request Form

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

08/27/24

Office of Equal Employment Opportunity

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
- [x] Existing DoD Information System
- [ ] 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.

Information collected includes name, DoD ID number, telephone number, email address, mailing address, and limited medical information. The collected information is used to support the Department of the Navy's reasonable accommodation process available to civilian employees and applicants for employment.

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)*

The information is used to determine the need for reasonable accommodations, type of reasonable accommodations needed, and to track estimated/actual cost of the reasonable accommodation.

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.

Completion of the form is voluntary. However, the agency may not be able to process or track the reasonable accommodation request without the information.

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

Individuals may consent to the use of their PII for the reasonable accommodation process by completing, signing and submitting the SECNAV 12306/1 Confirmation of Reasonable Accommodation Request Form.

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.)*

- [x] Privacy Act Statement
- [ ] Privacy Advisory
- [ ] Not Applicable

Authority: 5 U.S.C. 301; 5 U.S.C. Chapters 11, 13, 29, 31, 33, 41, 43, 51, 53, 55, 61, 63, 72, 75, 83, 99; 5 U.S.C. 7201; 29 USC 791; 10 U.S.C. 136;
E.O. 9830, as amended; 29 U.S.C. 79; 29 C.F.R. 1614.601, EEO Group Statistics; 29 CFR 1630.14, Medical Examinations and Inquiries Specifically Permitted; SECNAV Instruction 12713.14, Equal Employment Opportunity; and E.O. 9397 (SSN), as amended, and System of Records Notice (SORN) N12293-1.
Purpose(s): To provide relevant officials with the information to track, monitor, review, and process requests for reasonable accommodation.

Routine Uses(s): In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records contained therein may specifically be disclosed outside the Department of Defense (DoD) as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To the appropriate officials for the purpose of processing or responding to the request for reasonable accommodation and/or decisions related to such request. To officials and employees of the Equal Employment Opportunity Commission and/or other appropriate third parties responsible for investigating or adjudicating any cases that may result from a reasonable accommodation request. To unions recognized as exclusive bargaining representatives under the Civil Service Reform Act of 1978, 5 U.S.C. §§ 7111 and 7114, the Merit Systems Protection Board, the Office of the Special Counsel, arbitrators, the Federal Labor Relations Authority, and other parties responsible for the administration of the Federal labor-management program for the purpose of processing any corrective actions, grievances, or conducting administrative hearings or appeals. To the Office of Personnel Management (OPM), Office of Workers' Compensation, and Department of Veterans Affairs for the purpose of addressing civilian pay and leave, benefits, retirement deduction, and any other obligations. To an employee's private treating physician and to medical personnel retained by the DON to provide medical services in connection with an employee's health or physical condition related to employment. To the Occupational Safety and Health officials when needed to perform their duties.
Disclosure: Completion of this form is voluntary; however, failure to provide the requested information may result in an inability to process your reasonable accommodation request.

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

[X] Within the DoD Component	Specify.	Department of the Navy (DON), Office of Equal Employment Opportunity (EEO); EEO Leaders and Practitioners within the DON's subordinate commands; Authorized Navy and USMC HR personnel
[ ] Other DoD Components	Specify.	
[X] Other Federal Agencies	Specify.	OPM
[ ] 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.	
[ ] 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)*

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

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

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

SECNAV 12306/1 Confirmation of Reasonable Accommodation Request 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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier N12293-1

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. DAA-GRS-2017-0007-0001

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

(3) Retention Instructions.

Destroy three years after employee separation from the agency or three years after all administrative or judicial proceedings are concluded, whichever is later.

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. 301; 5 U.S.C. Chapters 11, 13, 29, 31, 33, 41, 43, 51, 53, 55, 61, 63, 72, 75, 83, 99; 5 U.S.C. 7201; 29 USC 791; 10 U.S.C. 136; E.O. 9830, as amended; 29 U.S.C. 79; 29 C.F.R. 1614.601, EEO Group Statistics; 29 CFR 1630.14, Medical Examinations and Inquiries Specifically Permitted; SECNAV Instruction 12713.14, Equal Employment Opportunity; and E.O. 9397 (SSN), as amended, and System of Records Notice (SORN) N12293-1.

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.

[X] 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.

OMB Control Number: OMB 0703-0063
Expiration: XX XXXXXXX 2025

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	

(a) Employment information: SF-172, Application for Federal Employment, Job Experience, Training, Performance Plans, Promotions, Reassignments, Adverse and Disciplinary actions;
(b) Education Information: DG-05 School Transcript, DG15-Employee Application, Certifications and Licensing;
(c) Other ID Number: Internal Employee ID Number, Manpower (TFMMS or TFSMS) Billet Number;
(d) Benefits Information: SF-2810 Notice of change in health and pay benefits, entitlements, SF-1152 Designation of Beneficiary, and Separation, Retirement;
(e) Emergency Contact Information: Name, relationship, address, phone, email.
(f) Financial Information: TSP Rate, TSP Dollar Amount, Annual Salary (Basic, Locality, Adjusted), Awards/Bonus', and Monetary Settlement Agreements.
(g) Disability Information: SF-256, Self-Identification of Disability; collects Name, Date of Birth, SSN, and Disability Code.

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 are not collected.

(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)*

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

(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
- ☒ Common Access Card (CAC)
- ☒ DoD Public Key Infrastructure Certificates
- ☒ Encryption of Data at Rest
- ☒ Encryption of Data in Transit
- ☒ External Certificate Authority Certificates
- ☒ Firewall
- ☒ Intrusion Detection System (IDS)
- ☒ Least Privilege Access
- ☒ Role-Based Access Controls
- ☒ Used Only for Privileged (Elevated Roles)
- ☒ User Identification and Password
- ☒ 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?

(a) HRCP only accessible from .mil, .gov., or authorized .edu authorized locations; validated via DISA.
(b) OCHR implemented CHRSAR form - multi-level authorization levels for approval to date; restricted to HR/Service Activities only. No modifications to form/access; users required to submit "new"; validates annual IA and PII training is active (w/in last year).

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

[X]	Yes, DITPR	DITPR System Identification Number	DITPR: 13428
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[X]	Yes, RMF tool	RMF tool Identification Number	2588
[ ]	No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

[X]	Authorization to Operate (ATO)	Date Granted:	3/3/2015
[ ]	ATO with Conditions	Date Granted:	
[ ]	Denial of Authorization to Operate (DATO)	Date Granted:	
[ ]	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

OCHR is presently in the process of renewing ATO; RMF/EMASS # 2588. Projected RMF transition date: XX XXX 20XX per the transition
POA&M.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

[X] Yes [ ] No

If "Yes," Enter UII 007-000002452 If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3]Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Meena Farzanfar	(1) Title	Department of the Navy (DON),, Disability Program Manager
(2) Organization	DON, Office of Equal Employment Opportunity (OEEO)	(3) Work Telephone	(202) 685-6238
(4) DSN		(5) E-mail address	meena.farzanfar@navy.mil
(6) Date of Review		(7) Signature	
b. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
c. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
d. Component Privacy Officer (CPO)	Dawn Noriega	(1) Title	Privacy Coordinator
(2) Organization		(3) Work Telephone	(202) 685-0412 EXT. 6533
(4) DSN		(5) E-mail address	dawn.noriega.ctr@us.navy.mil
(6) Date of Review		(7) Signature	

e. Component Records Officer	Tonya Price	(1) Title	Directives, Forms, and Information Collections Manager
(2) Organization	DON/AA, Directives and Records Management Division	(3) Work Telephone	(703) 693-9896
(4) DSN		(5) E-mail address	tonya.price1@navy.mil
(6) Date of Review		(7) Signature	
f. Component Senior Information Security Officer or Designee Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review:		(7) Signature	
g. Senior Component Official for Privacy (SCOP) or Designee Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
h. Component CIO Reviewing Official Name	Steve Daughety	(1) Title	DON Privacy Lead
(2) Organization	DON, Office of the Chief Information Officer (OCIO)	(3) Work Telephone	703-697-0045
(4) DSN		(5) E-mail address	steve.daughety1@navy.mil
(6) Date of Review	09/01/21	(7) Signature	

Publishing: Only Section 1 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: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

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 Section 1.