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 Sexual Assault Advocate Certification Program

2. DOD COMPONENT NAME:

Defense Human Resources Activity

3. PIA APPROVAL DATE:

Sexual Assault Prevention and Response Office (SAPRO)

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
- [x] From Federal employees and/or Federal contractors
- [ ] 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.

To track the certification of SARC and SAPR VAs. Information will be used to review, process, and report on the status of SARC and SAPR VA certification to Congress.

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)*

Identification and verification.

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.

SARCs and SAPR VAs may object to the collection of their PII by not submitting their PII on the required forms. However, they may not be considered qualified to perform their duties as a SARC and SAPR VA if they do not submit the information required to become certified.

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.

Applicants cannot give or withhold their consent to specific uses or their PII. The PII will be used in very limited ways, including to process and grant certification and communicate to the applicants and the DoD on certification statuses.

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

DD Form 2950, Department of Defense Sexual Assault Advocate Certification Program New Application Packet and DD Form 2950-1, Department of Defense Sexual Assault Advocate Certification Program Renewal Application Packet, includes a Privacy Act Statement on the first page as follows:

Authority: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Instruction 6495.03, Defense Sexual Assault Advocate Certification Program (D-SAACP).

Principal Purpose(s): To review and process applications for Sexual Assault Response Coordinator (SARC) and Sexual Assault Prevention Representative (SAPR) Victim Advocate (VA) certification.

Routine Use(s): To the Department of Justice, Justice Programs, Office for Victims of Crime, for the purpose of verifying certified Sexual Assault Response Coordinators (SARCs) and SAPR Victim Advocates (VAs) for participation in Advance Military Sexual Assault Advocate Online Training. See the applicable system of records notice for other routine uses located at: http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570562/dhra-10-dod/

DISCLOSURE: Voluntary. However, if you are a SARC or SAPR VA and do not complete this form to become certified, you may be disqualified from the position. 10 U.S.C. 1561, note requires DoD to establish a certification program.

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.	Defense Manpower Data Center
[X]	Other DoD Components	Specify.	Air Force, Army, Marine Corps, Navy, and National Guard
[X]	Other Federal Agencies	Specify.	Department of Justice-Office of Justice Programs, Office for Victims of Crimes
[ ]	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	[ ]	Databases
[ ]	Existing DoD Information Systems	[ ]	Commercial Systems
[ ]	Other Federal Information Systems		

Individual, via DD Form 2950 and DD Form 2950-1

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

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

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 10 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 10/30/17

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. GRS 1, Item 29a(1)

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

(3) Retention Instructions.

Temporary, Destroy when 5 years old or 5 years after completion of a specific training program (GRS 1, Item 29a(1)).

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 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; and DoD Instruction 6495.03, Defense Sexual Assault Advocate Certification Program (D-SAACP)

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.

The Unrestricted Reports of Sexual Assault and the 8-day report do not require licensing with a report control symbol in accordance with section 8 of Enclosure 3 of Volume 1 of DoD Manual 8910.01.

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	

Position type (DoD personnel); Service/DoD affiliation and status; grade/rank; installation/command; work email address and telephone number; official military address of applicant and applicant's SARC (commanding officer, street, city, state, ZIP code, country); position level (Level I, II, III, or IV); certificates of training; date of application; verification of sexual assault victim advocacy experience (position, dates, hours, supervisor; name, title, and work telephone number of verifier); evaluation of sexual assault victim experience (description of applicant skills, abilities, and experience; name, title, and office of evaluator), letters of recommendation by the first person in the chain of command, SARC, and the Senior Commander or the Commander; supervisor and commander statement of understanding, documentation of continuing education training courses; Defense Sexual Assault Advocate Certification Program (D-SAACP) identification (ID) number.

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.

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

Records are maintained in a controlled facility that employs physical restrictions such as double locks and is accessible only to authorized persons who hold key fobs. The data server is locked in a windowless room with restricted access. Additionally, all backups are physically stored in an off-site in a secure location. Paper files are stored in a locked filing cabinet in a locked room in the controlled facility.

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

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

Access to electronic data files in the system is role-based, restricted to essential personnel only, and requires two factor authentication. All data is backed-up daily, encrypted, and stored on an encrypted hard drive.

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

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

Data is maintained in a secure database on encrypted servers. System access to case files is limited to computers within a closed network, not connected to the internet or other server.

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

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]?

☐	Yes, DITPR	DITPR System Identification Number	
☐	Yes, SIPRNET	SIPRNET Identification Number	
☐	Yes, RMF tool	RMF tool Identification Number	
☒	No		

If "No," explain.

D-SAACP is a COTs office automation based system.

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:

☐	Authorization to Operate (ATO)	Date Granted:	
☐	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.

RMF Assessment pending with ECD of Dec 2017.

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

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?

☐ Yes ☒ No

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

[3]Guidance on Risk Management Framework (RMF) tools (i.e., 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	Bette M.S. Inch	(1) Title	Senior Victim Assistant Advisor
(2) Organization	DoD Sexual Assault Prevention and Response Office	(3) Work Telephone	571-372-2656
(4) DSN		(5) E-mail address	bette.m.inch.civ@mail.mil
(6) Date of Review	10/26/17	(7) Signature	INCH.BETTE.MS.1228783176 Digitally signed by INCH.BETTE.M S.1228783176 Date: 2017.10.26 12:14:47 -04'00'
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)	Judy Montoya	(1) Title	Privacy Officer
(2) Organization	Chief Information Office Headquarters Defense Human Resources Activity	(3) Work Telephone	571-372-7390
(4) DSN		(5) E-mail address	judith.e.montoya.civ@mail.mil
(6) Date of Review	10/27/17	(7) Signature	MONTOYA.JUDITH.ESTELLE.1157331503 Digitally signed by MONTOYA.JUDITH.ESTELLE.1157331503 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=MONTOYA.JUDITH.ESTELLE.1157331503 Date: 2017.10.27 14:18:31 -04'00'

e. Component Records Officer	Retta Graham-Hall	(1) Title	Records Manager
(2) Organization	Chief Information Office Headquarters Defense Human Resources Activity	(3) Work Telephone	571-372-1785
(4) DSN		(5) E-mail address	retta.h.graham-hall.civ@mail.mil
(6) Date of Review	10/27/17	(7) Signature	GRAHAM-HALL.RETTA.H.1229140074 Digitally signed by GRAHAM-HALL.RETTA.H.1229140074 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=GRAHAM-HALL.RETTA.H.1229140074 Date: 2017.10.27 12:15:54 -04'00'
f. Component Senior Information Security Officer or Designee Name	Cheryl Dallas	(1) Title	Cybersecurity Manager
(2) Organization	Chief Information Office Headquarters Defense Human Resources Activity	(3) Work Telephone	571-372-1069
(4) DSN		(5) E-mail address	cheryl.l.dallas.civ@mail.mil
(6) Date of Review:	10/27/2017	(7) Signature	DALLAS.CHERYL.LYNN.1049433189 Digitally signed by DALLAS.CHERYL.LYNN.1049433189 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=DALLAS.CHERYL.LYNN.1049433189 Date: 2017.10.27 08:15:52 -04'00'
g. Senior Component Official for Privacy (SCOP) or Designee Name	Mary V. Short	(1) Title	Senior Privacy Analyst
(2) Organization	WHS/ESD OSD/JS Privacy Office	(3) Work Telephone	571-372-0444
(4) DSN		(5) E-mail address	mary.v.short.civ@mail.mil
(6) Date of Review	10/30/17	(7) Signature	SHORT.MARY.V.1229496880 Digitally signed by SHORT.MARY.V.1229496880 Date: 2017.10.30 13:46:41 -04'00'
h. Component CIO Reviewing Official Name	Katrina Logan	(1) Title	Chief Information Officer
(2) Organization	Chief Information Office Headquarters Defense Human Resources Activity	(3) Work Telephone	571-372-2005
(4) DSN		(5) E-mail address	katrina.l.logan4.civ@mail.mil
(6) Date of Review	10/31/17	(7) Signature	LOGAN.KATRINA.LYNN.1269500871 Digitally signed by LOGAN.KATRINA.LYNN.1269500871 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=LOGAN.KATRINA.LYNN.1269500871 Date: 2017.10.31 12:02:03 -04'00'

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.